

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-314835

(43)Date of publication of application : 29.11.1996

(51)Int.Cl.

G06F 13/00

G06F 11/30

H04Q 9/00

H04Q 9/00

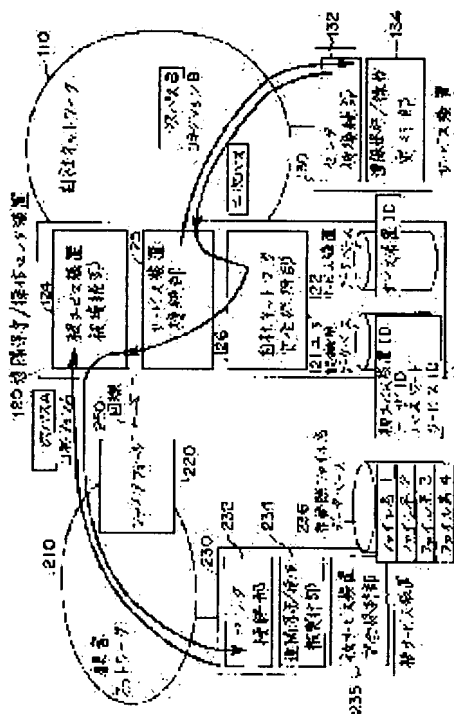
(21)Application number : 07-121975

(71)Applicant : FUJITSU LTD

(22)Date of filing : 19.05.1995

(72)Inventor : TANNO IPPEI

(54) DEVICE TO RECEIVE SERVICE, CENTER DEVICE, SERVICE DEVICE AND REMOTE CONTROL SYSTEM



(57)Abstract:

PURPOSE: To execute remote control between a service device and a device to receive service connected to an internal network where fire walls are mutually installed.

CONSTITUTION: The device 230 to receive service establishes connection A with a remote maintenance/control center device 120 through a customer network 210 and a fire wall 220. Next, the device 230 to receive service transmits security check information through the connection A to the remote maintenance/ control center device 120. The remote maintenance/control center device 120 checks this security check information by retrieving a data base 121 for user certification and when it is confirmed that the contracted user owns the device 230 to receive service, connection B with the service device 130 is established through its own company network 110. Thus, the service

device 130 can remotely maintain/control the device 230 to receive service through a logical path composed of the connection A and the connection B.

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平8-314835

(43)公開日 平成8年(1996)11月29日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 13/00	3 5 1	7368-5E	G 0 6 F 13/00	3 5 1 Z
		7313-5B	11/30	D
H 0 4 Q 9/00	3 0 1		H 0 4 Q 9/00	3 0 1 Z
	3 2 1			3 2 1 Z

審査請求 未請求 請求項の数20 O L (全 31 頁)

(21)出願番号 特願平7-121975

(22)出願日 平成7年(1995)5月19日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 丹野 一平

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人 弁理士 大菅 義之 (外1名)

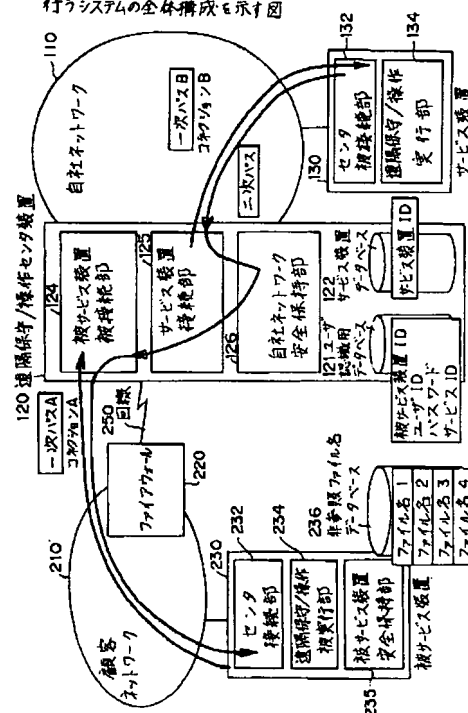
(54)【発明の名称】 被サービス装置、センタ装置、サービス装置、及び遠隔操作システム

(57)【要約】

【目的】 本発明は、互いにファイアウォールが設置されている内部ネットワークに接続されたサービス装置と被サービス装置との間で、遠隔操作を実施できるようにすることを目的とする。

【構成】 被サービス装置230は、顧客ネットワーク210及びファイアウォール220を介して遠隔保守/操作センタ装置120とコネクションAを確立する。次に、被サービス装置230は、該コネクションAを介して遠隔保守/操作センタ装置120にセキュリティ・チェック情報を送信する。遠隔保守/操作センタ装置120は、このセキュリティ・チェック情報をユーザ認証用データベース121を検索してチェックし、上記被サービス装置230が契約先のユーザのものであると確認した場合には、自社ネットワーク110を介してサービス装置130とコネクションBを確立する。これにより、サービス装置130は、上記コネクションAとコネクションBによって構成される論理的なパスを介して、被サービス装置230を遠隔保守/操作することができるようになる。

本発明の一実施例である遠隔保守及び遠隔操作を行うシステムの全体構成を示す図



【特許請求の範囲】

【請求項1】 外部ネットワークに対する第一のファイアウォールが設置された遠隔操作サービス提供者者の内部ネットワークに接続されたサービス装置によって、該外部ネットワークを介して遠隔操作サービスを実施される、該外部ネットワークに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファイアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信するパケット通信手段と、

該パケット通信手段が受信したパケットから遠隔操作の指示情報を取り出し、該指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、
を備えたことを特徴とする被サービス装置。

【請求項2】 外部ネットワークに対する第一のファイアウォールが設置された遠隔操作サービス提供者者の内部ネットワークに接続されたサービス装置によって、該外部ネットワークを介して遠隔操作サービスを実施される、該外部ネットワークに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第二のファイアウォールを介して前記第一のファイアウォールとの間にコネクションを確立し、該コネクションを介して該第一のファイアウォールとの間でパケットを送受信するパケット通信手段と、

該パケット通信手段によって受信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックするセキュリティ・チェック手段と、

該セキュリティ・チェック手段によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、

該遠隔操作実行手段によって実行された遠隔操作の実行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する実行結果返信手段と、

を備えたことを特徴とする被サービス装置。

【請求項3】 インターネットに対する第一のファイアウォールが設置された遠隔操作サービス提供者者の内部ネットワークに接続されたサービス装置によって、該インターネットを介して遠隔操作サービスを実施される、該インターネットに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファ

イアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信するパケット通信手段と、

該パケット通信手段が受信したパケットから遠隔操作の指示情報を取り出し、該指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、
を備えたことを特徴とする被サービス装置。

【請求項4】 インターネットに対する第一のファイアウォールが設置された遠隔操作サービス提供者者の内部ネットワークに接続されたサービス装置によって、該インターネットを介して遠隔操作サービスを実施される、該インターネットに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第二のファイアウォールを介して前記第一のファイアウォールとの間にコネクションを確立し、該コネクションを介して該第一のファイアウォールとの間でパケットを送受信するパケット通信手段と、

該パケット通信手段によって受信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックするセキュリティ・チェック手段と、

該セキュリティ・チェック手段によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、

該遠隔操作実行手段によって実行された遠隔操作の実行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する実行結果返信手段と、

を備えたことを特徴とする被サービス装置。

【請求項5】 外部ネットワークに対する第一のファイアウォールが設置された契約先のユーザの内部ネットワークに接続された被サービス装置に対して、該外部ネットワークを介して遠隔操作サービスを実施する業者の内部ネットワークの該外部ネットワークに対する第二のファイアウォールとして機能するセンタ装置において、

前記第一のファイアウォールと前記外部ネットワークを介して前記被サービス装置との間に第一のコネクションを確立し、該第一のコネクションを介して前記被サービス装置との間でパケットを送受信する第一のパケット通信手段と、

前記第一のコネクションが確立された後に、該第一のパケット通信手段によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックするセキュリティ・チェック手段と、

該セキュリティ・チェック手段によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二のコネクションを確立し、該第二のコネクションを介して前記

自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する第二のパケット通信手段と、を備えたことを特徴とするセンタ装置。

【請求項6】 契約先のユーザの認証情報が登録されたデータベースをさらに備え、

前記セキュリティ・チェック手段は、前記受信パケットに該データベースに登録されている認証情報が格納されているか否かをチェックすることにより、前記受信パケットが契約先のユーザからのものであるか否かを判断すること、

を特徴とする請求項5記載のセンタ装置。

【請求項7】 前記第二のコネクションを確立するために使用するサービス装置の識別情報が登録されたデータベースをさらに備え、

前記第二のパケット通信手段は、前記第一のパケット通信手段によって受信されたパケットに格納されているサービス識別情報に対応するサービス装置識別情報を前記第二のデータベースから取り出し、このサービス装置識別情報を用いて前記第二のコネクションを確立すること、

を特徴とする請求項5記載のセンタ装置。

【請求項8】 インターネットに対する第一のファイアウォールが設置された契約先のユーザの内部ネットワークに接続された被サービス装置に対して、該外部ネットワークを介して遠隔操作サービスを実施する業者の内部ネットワークの該インターネットに対する第二のファイアウォールとして機能するセンタ装置において、

インターネットに対する第一のファイアウォールが設置された遠隔操作サービス提供者の内部ネットワークに接続されたサービス装置に対して、該インターネットを介して遠隔操作サービスを実施する業者の内部ネットワークの該インターネットに対する第二のファイアウォールとして機能するセンタ装置において、

前記第一のファイアウォールと前記インターネットを介して前記被サービス装置との間に第一のコネクションを確立し、該第一のコネクションを介して前記被サービス装置との間でパケットを送受信する第一のパケット通信手段と、

前記第一のコネクションが確立された後に、該第一のパケット通信手段によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックするセキュリティ・チェック手段と、

該セキュリティ・チェック手段によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二のコネクションを確立し、該第二のコネクションを介して前記自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する第二のパケット通信手段と、

を備えたことを特徴とするセンタ装置。

【請求項9】 契約先のユーザの認証情報が登録されたデータベースをさらに備え、

前記セキュリティ・チェック手段は、前記受信パケットに該データベースに登録されている認証情報が格納されているか否かをチェックすることにより、前記受信パケットが契約先のユーザからのものであるか否かを判断すること、

を特徴とする請求項8記載のセンタ装置。

10 【請求項10】 前記第二のコネクションを確立するために使用するサービス装置のIPアドレスが登録されたデータベースをさらに備え、

前記第二のパケット通信手段は、前記第一のパケット通信手段によって受信されたパケットに格納されているサービス識別情報に対応するIPアドレスを前記第二のデータベースから取り出し、このIPアドレスを用いて前記第二のコネクションを確立すること、

を特徴とする請求項8記載のセンタ装置。

20 【請求項11】 外部ネットワークに対して第一のファイアウォールが設置された顧客の内部ネットワークに接続された被サービス装置に対して遠隔操作サービスを実施する、上記外部ネットワークに対して第二のファイアウォールが設置された自社の内部ネットワークに接続されたサービス装置において、

前記第二のファイアウォールとコネクションを確立し、該コネクションを介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信するパケット通信手段と、

30 該パケット通信手段によって受信されたパケットに格納されている遠隔操作の指示情報によって指示される遠隔操作を、被サービス装置に対して実施するためのコマンドが設定されたパケットを生成し、このパケットを、前記パケット通信手段を介して、前記第二のファイアウォールに送信する遠隔操作実行手段と、

を備えることを特徴とするサービス装置。

【請求項12】 前記遠隔操作実行手段は、前記パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力すること、を特徴とする請求項11記載のサービス装置。

【請求項13】 インターネットに対して第一のファイアウォールが設置された顧客の内部ネットワークに接続された被サービス装置に対して遠隔操作サービスを実施する、上記インターネットに対して第二のファイアウォールが設置された自社の内部ネットワークに接続されたサービス装置において、

前記第二のファイアウォールとコネクションを確立し、該コネクションを介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信するパケット通信手段と、

該パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の指示情報を取り出し、該指示情報によって指示される遠隔操作を実施するためのコマンドが設定されたパケットを生成し、このパケットを前記第二のファイアウォールに送信する遠隔操作実行手段と、
を備えることを特徴とするサービス装置。

【請求項14】 前記遠隔操作実行手段は、前記パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力すること、を特徴とする請求項13記載のサービス装置。

【請求項15】 顧客の内部ネットワークと遠隔操作を提供する業者の内部ネットワークが外部ネットワークを介して接続されており、かつ、上記二つの内部ネットワークに対して前記外部ネットワークに対するファイアウォールが設置されているシステムを利用して、上記顧客の内部ネットワークに接続された被サービス装置を、上記遠隔操作を提供する業者の内部ネットワークに接続されたサービス装置によって遠隔操作するサービスを実施する遠隔操作サービスシステムにおいて、

前記被サービス装置は、
前記顧客ネットワーク及び該顧客ネットワークに対する第一のファイアウォールを介して、前記遠隔操作サービス提供業者の内部ネットワークに対して設置された第二のファイアウォールに第一のコネクションを確立し、該第一のコネクションを介して前記遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置と遠隔操作を実施するためのデータが格納されているパケットを送受信し、

前記第二のファイアウォールは、
前記被サービス装置と前記第一のコネクションを確立した後に、自社の内部ネットワークを介して前記サービス装置と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置と前記サービス装置との間で授受されるパケットを中継し、
前記サービス装置は、

前記被サービス装置との間で授受するパケットを、前記第二のファイアウォールと前記第二のコネクションを介して送受信することにより、前記被サービス装置に対して遠隔操作のサービスを実施すること、
を特徴とする遠隔操作サービスシステム。

【請求項16】 前記第二のファイアウォールは、
前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置が送信してくるパケットに設定されているデータの内容を基に、前記被サービス装置が契約先のユーザのものであるか否かを認証する認証手段を、
を備えることを特徴とする請求項15記載の遠隔操作サービスシステム。

【請求項17】 前記被サービス装置は、
前記第二のファイアウォールから、前記第一のコネクションを介して前記サービス装置から送信されてきたパケットを受信した際に、そのパケットに格納されている遠隔操作実行用のコマンドが正当なコマンドであるか否かを認証する認証手段を、

を備えることを特徴とする請求項15記載の遠隔操作実行システム。を備えることを特徴とするサービス装置。

【請求項18】 顧客の内部ネットワークと遠隔操作を提供する業者の内部ネットワークがインターネットを介して接続されており、かつ、上記二つの内部ネットワークに対して前記インターネットに対するファイアウォールが設置されているシステムを利用して、上記顧客の内部ネットワークに接続された被サービス装置を、上記遠隔操作を提供する業者の内部ネットワークに接続されたサービス装置によって遠隔操作するサービスを実施する遠隔操作サービスシステムにおいて、

前記被サービス装置は、
前記顧客ネットワーク及び該顧客ネットワークに対する第一のファイアウォールを介して、前記遠隔操作サービス提供業者の内部ネットワークに対して設置された第二のファイアウォールに第一のコネクションを確立し、該第一のコネクションを介して前記遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置と遠隔操作を実施するためのデータが格納されているパケットを送受信し、

前記第二のファイアウォールは、
前記被サービス装置と前記第一のコネクションを確立した後に、自社の内部ネットワークを介して前記サービス装置と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置と前記サービス装置との間で授受されるパケットを中継し、
前記サービス装置は、

前記被サービス装置との間で授受するパケットを、前記第二のファイアウォールと前記第二のコネクションを介して送受信することにより、前記被サービス装置に対して遠隔操作のサービスを実施すること、
を特徴とする遠隔操作サービスシステム。

【請求項19】 前記第二のファイアウォールは、
前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置が送信してくるパケットに設定されているデータの内容を基に、前記被サービス装置が契約先のユーザのものであるか否かを認証する認証手段を、

を備えることを特徴とする請求項18記載の遠隔操作サービスシステム。

【請求項20】 前記被サービス装置は、
前記第二のファイアウォールから、前記第一のコネクションを介して前記サービス装置から送信されてきたパケットを受信した際に、そのパケットに格納されている遠

隔操作実行用のコマンドが正当なコマンドであるか否かを認証する認証手段を、
備えることを特徴とする請求項18記載の遠隔操作実行システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、インターネットなどのオープンな外部ネットワークを介して、ユーザ側のネットワークに接続された装置を、自社内のネットワークに接続されたサービス装置によって遠隔操作しながら保守・管理等を行う遠隔操作方式に係わり、特に、互いのネットワークに対してファイアウォールが設けられている場合における遠隔操作方式に関する。

【0002】

【従来の技術】最近では、出張経費及びそれに伴う時間の節約などのために、ユーザの装置の保守や管理作業を、ネットワークを介して、遠隔操作により行う方式が盛んになりつつある。

【0003】また、この遠隔操作のためのネットワークとしてインターネットを利用する方式の採用も試みられるようになってきている。インターネットは、世界的なネットワークであり、世界中の不特定の相手と自由に通信することが可能である。したがって、インターネットを利用することにより、グローバルな遠隔保守作業が可能となる。

【0004】ところで、インターネットは、オープンなネットワークであるがために、セキュリティの点で問題がある。特に、企業が社内ネットワークをインターネットに接続する場合、該社内ネットワークに接続された全てのホストがインターネットを介して部外者からアクセス可能となるので、極秘すべき重要な内部情報が盗まれたり、システムがクラッシュさせられたり、さらにはデータが変更させられるなどの危険にさらされることになる。

【0005】このため、最近では、インターネットと社内ネットワークとの間に”ファイアウォール”を設けるようになってきている。ファイアウォールは、不法な侵入者から社内ネットワークを保護するための機構であり、一般に、パケットフィルタリングゲートウェイ、サーキットゲートウェイ、及びアプリケーションゲートウェイに大別される。

【0006】図j1は、外部ネットワーク（インターネット）1と内部ネットワーク2（社内ネットワーク）との間に設置された上記パケットフィルタリングゲートウェイ機能を備えたファイアウォール3の概略構成を示す図である。同図には、IPアドレス・フィルタリングとTCPポート・フィルタリングの例が示されている。

【0007】インターネット上の通信は、TCP/IPプロトコルをベースにして行われており、IPデータグラム（IPパケット）がインターネット内をパケットリ

ーの形でルーティング制御される。該IPデータグラムは、そのヘッダ部分にIPヘッダとTCPヘッダを含んでいる。

【0008】IPヘッダは、IP宛先アドレス（図中の受信IPアドレス）とIP送信元アドレス（図中の発信IPアドレス）を含んでいる。このIPアドレスは、ネットワーク・アドレスとホスト・アドレスから構成されている。

【0009】また、TCPヘッダは、受信ポート番号と発信ポート番号を含んでいる。このポート番号はプロセスに1対1に対応するもので、インターネットを介したプロセス間通信に利用される。

【0010】ファイアウォール3は、その内部にIPアドレス登録テーブル32とポート番号登録テーブル34を備えている。IPアドレス登録テーブル32には、内部ネットワーク2に通過させてもよいIPアドレスの組が登録されている。また、ポート番号登録テーブル34には、内部ネットワーク2に通過させてもよいポート番号の組が登録されている。

【0011】上記IPアドレス・フィルタリングでは、パケットを受信すると、上記IPアドレス登録テーブル32を参照して、そのパケットのIPデータグラムに、テーブル32に登録されていない発信IPアドレスがIPヘッダに設定されているIPデータグラムを棄却する。また、TCPポート・フィルタリングでは、IPデータグラム（パケット）を受信すると、上記ポート番号登録テーブル34を参照して、そのテーブル34に登録されていないポート番号の組がTCPヘッダに設定されているIPデータグラムを棄却する。これにより、Telnet、FTPなどの特定のアプリケーションをフィルタリングできる。

【0012】また、図j2は、ファイアウォール3の第2の機能を説明する図である。ファイアウォール3は、外部ネットワーク1（インターネットなど）上のホストが、内部ネットワーク2内のホスト（内部ホスト）を直接アクセスできないようにするために、内部ネットワーク2内のホストのアクセスを代行する機能を備えている。すなわち、内部ネットワーク2内のホストが外部ネットワーク1にアクセスする際には、常に、ファイアウォール3を介して行うようにする。

【0013】同図の例では、ファイアウォール3に対して、“E”のIPアドレスが設定されている。また、内部ネットワーク2内の各ホストA、B、C、及びDに対して、それぞれ、“A”、“B”、“C”、及び“D”のIPアドレスが設定されている。このようなシステムにおいて、ホストBが外部ネットワーク1上のあるホスト（外部ホスト）に対してIPデータグラム12を送信する場合、このIPデータグラム12をファイアウォール3に送信する。したがって、このIPデータグラム12の発信IPアドレスは“B”に設定される。ファイア

ウォール3は、このIPデータグラム12を受信すると、その発信IPアドレスを、自己のIPアドレスである”E”に変換して、外部ネットワーク1に送出する。

【0014】このように、外部ネットワーク1に対してはファイアウォール3のみを公開するようにして、内部ネットワーク2の存在を外部ネットワーク1に知らせないようにする。尚、この機能はIP中継機能とも呼ばれる。

【0015】以上述べたようなパケットフィルタリングゲートウェイ機能を備えたファイアウォール3を内部ネットワーク2と外部ネットワーク1との間に設置することにより、外部ネットワーク1を介して、直接、内部ネットワーク2内に侵入しようとする不法なIPデータグラムを、ほぼ完全にブロックすることが可能になる。

【0016】図j3は、A社、B社、C社、及びD社のネットワーク2A、2B、2C、および2Dが商用インターネット5に接続されたシステムを示す図である。このシステムにおいて、A社、B社、C社、及びD社は、それぞれの内部ネットワーク2A、2B、2C、および2Dを、商用インターネット5を介する外部からの不法アクセスから守るために、該商用インターネット5と自社の内部ネットワーク2A、2B、2C、および2Dとの間にファイアウォール3A、3B、3C、及び3Dを設置している。

【0017】

【発明が解決しようとする課題】次に、上記図j3に示すようなシステムにおいて発生する問題点を、図j4を参照しながら説明する。

【0018】図j4において、A社が顧客が運営するネットワーク内の装置やソフトウェアなどに対する保守や作業代行などのサービスを実施する会社であり、該顧客先がD社であったとする。この場合、A社が自社ネットワークに接続されたサービス装置6を用いて、D社のネットワーク2Dに接続された被サービス装置7の保守や作業代行を、商用インターネット5を介する遠隔操作により実施したいと考えたとする。

【0019】この場合、A社のサービス装置6が商用インターネット5を介して、D社の被サービス装置7に該遠隔操作用のパケットを送信しても、例えばA社のファイアウォール3AのIPアドレスが、D社のファイアウォール3DのIPアドレス登録テーブル32に登録されていない場合には、上記サービス装置6がD社のファイアウォール3Dに送信したパケットは、ファイアウォール3Dによって棄却されてしまい、D社の内部ネットワーク2Dに入り込むことができない。このため、A社ではD社の被サービス装置7に対して保守や作業代行等のサービスを実施することができない。

【0020】また、D社のファイアウォール3DのIPアドレス登録テーブル32に、A社のファイアウォール3AのIPアドレスを登録すれば、A社のサービス装置

6がD社の被サービス装置7を遠隔操作して、その装置7の保守や作業を実行できるようになるが、これは、セキュリティの点で問題がある。すなわち、この場合、A社のサービス装置6以外のホストを操作することにより、D社の内部ネットワーク2Dのシステムを破壊したり、重要な情報を盗まれる可能性がある。何故ならば、D社のファイアウォール3Dは、商用インターネット5を介して受信するA社のファイアウォール3Aから送られてくるパケットを、A社のいずれのホストが発信したパケットであるか特定できないからである。

【0021】このため、従来は、図j5に模式的に示すように、公衆回線8または専用線により、A社のサービス装置6と顧客であるD社の被サービス装置7を、直接二点間接続して、被サービス装置7の保守や作業代行を実施していた。しかしながら、このような方式を用いると、A社及びD社が共に、該直接二点間接続するための専用の通信装置9A、9Dなどの装備やサービス授受専用の環境を用意する必要があり、両社が二重投資をせねばならずコストの増大をもたらし、好ましくない。また、さらに、サービス実施時には、社内のネットワークのセキュリティを保持するために、サービス装置6と被サービス装置7とも、それぞれの社内ネットワーク2A、2Dから切り離し、サービスが終了した時点で、再び、それらの装置6、7をそれぞれの社内ネットワーク2A、2Dに接続するという煩雑な作業が必要となる。

【0022】本発明は、互いにファイアウォールを設置している遠隔操作により保守や管理サービスを実施する会社と該サービスを受ける会社の双方が、自社のネットワークのセキュリティを保持しつつ、安価な設備投資で、遠隔保守や遠隔操作を実施できるシステムを実現することを目的とする。

【0023】

【課題を解決するための手段】図1は本発明の原理を説明する図（その1）である。図1に示す発明（第一の発明）は、外部ネットワークに対する第一のファイアウォールが設置された遠隔操作サービス提供者の内部ネットワークに接続されたサービス装置によって、該外部ネットワークを介して遠隔操作サービスを実施される、該外部ネットワークに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置を前提とする。

【0024】パケット通信手段51は、前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファイアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信するまた、第二の発明は、上記パケット通信手段51と遠隔操作実行手段52に加え、さらに、遠隔操作実行手段52によって実行された遠隔操作の実

行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する実行結果返信手段53と、該パケット通信手段51によって受信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックするセキュリティ・チェック手段54を備える。この場合、遠隔操作実行手段52は、セキュリティ・チェック手段54によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する。

【0025】前記第一及び第二の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。図2は、本発明の原理を説明する図（その2）である。

【0026】この図2に示す第三の発明は、外部ネットワークに対する第一のファイアウォールが設置された契約先のユーザの内部ネットワークに接続された被サービス装置に対して、該外部ネットワークを介して遠隔操作サービスを実施する業者の内部ネットワークの該外部ネットワークに対する第二のファイアウォールとして機能するセンタ装置を前提とする。

【0027】第一のパケット通信手段61は、前記第一のファイアウォールと前記外部ネットワークを介して前記被サービス装置との間に第一の接続を確立し、該第一の接続を介して前記被サービス装置との間でパケットを送受信する。

【0028】セキュリティ・チェック手段62は、前記第一の接続が確立された後に、第一のパケット通信手段61によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックする。

【0029】第二のパケット通信手段63は、セキュリティ・チェック手段62によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二の接続を確立し、該第二の接続を介して前記自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する。

【0030】また、上記第三の発明において、契約先のユーザの認証情報が登録されたデータベースをさらに備え、前記セキュリティ・チェック手段62は、前記受信パケットに該データベースに登録されている認証情報が格納されているか否かをチェックすることにより、前記受信パケットが契約先のユーザからのものであるか否かを判断するような構成にしてもよい。

【0031】また、上記第三の発明において、前記第二の接続を確立するために使用するサービス装置の識別情報が登録されたデータベースをさらに備え、前記第二のパケット通信手段63は、前記第一のパケット通信手段61によって受信されたパケットに格納されているサービス識別情報に対応するサービス装置識別情報

を前記第二のデータベースから取り出し、このサービス装置識別情報を用いて前記第二の接続を確立するような構成にしてもよい。

【0032】また、前記第三の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。図3は、本発明の原理を説明する図（その3）である。

【0033】この図3に示す第四の発明は、外部ネットワークに対して第一のファイアウォールが設置された顧客の内部ネットワークに接続された被サービス装置に対して遠隔操作サービスを実施する、上記外部ネットワークに対して第二のファイアウォールが設置された自社の内部ネットワークに接続されたサービス装置を前提とする。

【0034】パケット通信手段71は、前記第二のファイアウォールと接続を確立し、該接続を介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信する。

【0035】遠隔操作実行手段71は、該パケット通信手段71によって受信されたパケットに格納されている遠隔操作の指示情報によって指示される遠隔操作を、被サービス装置に対して実施するためのコマンドが設定されたパケットを生成し、このパケットを、前記パケット通信手段を介して、前記第二のファイアウォールに送信する。

【0036】上記第四の発明において、例えば、前記遠隔操作実行手段72は、前記パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力する。

【0037】前記第四の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。図4は、本発明の原理を説明する図（その4）である。

【0038】この図5に示す第五の発明は、顧客の内部ネットワーク82と遠隔操作を提供する業者の内部ネットワーク86が外部ネットワーク84を介して接続されており、かつ、上記二つの内部ネットワーク82、86に対して前記外部ネットワーク84に対するファイアウォール83、85が設置されているシステムを利用して、上記顧客の内部ネットワーク82に接続された被サービス装置81を、上記遠隔操作を提供する業者の内部ネットワーク86に接続されたサービス装置87によって遠隔操作するサービスを実施する遠隔操作サービスシステムを前提とする。

【0039】そして、前記被サービス装置81は、前記顧客ネットワーク82及び該顧客ネットワーク82に対する第一のファイアウォール83を介して、前記遠隔操作サービス提供業者の内部ネットワーク86に対して設置された第二のファイアウォール85に第一の接続を確立し、該第一の接続を介して前記遠隔操作サービス提供業者の内部ネットワーク86に接続さ

れたサービス装置87と遠隔操作を実施するためのデータが格納されているパケットを送受信し、前記第二のファイアウォール85は、前記被サービス装置81と前記第一のコネクションを確立した後に、自社の内部ネットワーク86を介して前記サービス装置87と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置81と前記サービス装置87との間で授受されるパケットを中継し、前記サービス装置87は、前記被サービス装置81との間で授受するパケットを、前記第二のファイアウォール85と前記第二のコネクションを介して送受信することにより、前記被サービス装置81に対して遠隔操作のサービスを実施することを特徴とする。

【0040】上記第五の発明において、前記第二のファイアウォール85は、例えば、前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置81が送信してくるパケットに設定されているデータの内容を基に、前記被サービス装置81が契約先のユーザのものであるか否かを認証する認証手段を、を備えるような構成にしてもよい。

【0041】また、上記第五の発明において、前記被サービス装置81は、前記第二のファイアウォール85から、前記第一のコネクションを介して前記サービス装置87から送信されてきたパケットを受信した際に、そのパケットに格納されている遠隔操作実行用のコマンドが正当なコマンドであるか否かを認証する認証手段を、備えるような構成にしてもよい。

【0042】前記第五の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。

【0043】

【作用】第一の発明では、パケット通信手段51が、前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファイアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信する。そして、遠隔操作実行手段52は、パケット通信手段51が受信したパケットから遠隔操作の指示情報を取り出し、該指示情報の指示に従って自装置の遠隔操作を実行する。

【0044】したがって、遠隔操作サービス提供者の内部ネットワークと顧客ネットワークが、互いに外部ネットワークに対してファイアウォールを設置している内部ネットワークに接続された被サービス装置は、遠隔操作サービス提供者の内部ネットワーク内部に自己が生成したパケットを送信できると共に、遠隔操作サービス提供者の内部ネットワークに接続されたサービス装置からパケットを受信できる。

【0045】また、第二の発明では、セキュリティ・チェック手段54が、該パケット通信手段51によって受

信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックする。そして、遠隔操作実行手段52は、セキュリティ・チェック手段54によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する。そして、実行結果返信手段53が、遠隔操作実行手段52によって実行された遠隔操作の実行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する。

【0046】したがって、被サービス装置は、その安全性を保持しながら、遠隔操作のサービスを受けることができる。また、サービス装置は、第一のファイアウォールを介して、被サービス装置において実施された遠隔操作の実行結果を得ることができる。

【0047】また、第三の発明では、第一のパケット通信手段61が、前記第一のファイアウォールと前記外部ネットワークを介して前記被サービス装置との間に第一のコネクションを確立し、該第一のコネクションを介して前記被サービス装置との間でパケットを送受信する。そして、セキュリティ・チェック手段62は、前記第一のコネクションが確立された後に、第一のパケット通信手段61によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックする。続いて、第二のパケット通信手段63は、セキュリティ・チェック手段62によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二のコネクションを確立し、該第二のコネクションを介して前記自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する。

【0048】したがって、第一のファイアウォールが設置されている顧客の内部ネットワークに接続された被サービス装置との間でパケットの送受信をすることができる。また、受信するパケットのセキュリティ・チェックを行い、不当なパケットを棄却することができる。そして、自社の内部ネットワークに接続されたサービス装置に正規の契約先のユーザの被サービス装置から送信されてきたパケットのみを送信することができる。また、上記サービス装置から上記顧客の被サービス装置に送られるパケットを、該被サービス装置に送信することができる。

【0049】また、第四の発明では、パケット通信手段71が、前記第二のファイアウォールとコネクションを確立し、該コネクションを介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信する。そして、遠隔操作実行手段72は、該パケット通信手段71によって受信されたパケットに格納されている遠隔操作の指示情報によって指示される遠隔操作を、被サービス装置に対して実施するためのコマンドを設定されたパケットを生成し、このパケットを、前記バ

ケット通信手段71を介して、前記第二のファイアウォールに送信する。また、さらに、例えば、前記遠隔操作実行手段72は、前記ケット通信手段71によって受信されたケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力する。

【0050】したがって、遠隔操作サービス提供者の内部ネットワークに接続されたサービス装置は、外部ネットワークに対して設置された第二のファイアウォールとケットを送受信することができる。このため、第二のファイアウォールが顧客の内部ネットワークに接続された被サービス装置との間にコネクションを確立することにより、上記サービス装置は、被サービス装置と遠隔操作のサービスを実施するためにケットを送受信することができる。

【0051】また、第五の発明では、被サービス装置81が、前記顧客ネットワーク82及び該顧客ネットワーク82に対する第一のファイアウォール83を介して、前記遠隔操作サービス提供者の内部ネットワーク86に対して設置された第二のファイアウォール85に第一のコネクションを確立し、該第一のコネクションを介して前記遠隔操作サービス提供者の内部ネットワーク86に接続されたサービス装置87と遠隔操作を実施するためのデータが格納されているケットを送受信する。

【0052】また、第二のファイアウォール85は、前記被サービス装置81と前記第一のコネクションを確立した後に、自社の内部ネットワーク86を介して前記サービス装置87と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置81と前記サービス装置87との間で授受されるケットを中継する。

【0053】さらに、サービス装置87は、前記被サービス装置81との間で授受するケットを、前記第二のファイアウォール85と前記第二のコネクションを介して送受信することにより、前記被サービス装置81に対して遠隔操作のサービスを実施する。

【0054】この場合、例えば、前記第二のファイアウォール85は、内部の認証手段により、前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置81が送信してくるケットに設定されているデータの内容を基に、前記被サービス装置81が契約先のユーザのものであるか否かを認証する。

【0055】また、例えば、前記被サービス装置81は、内部の認証手段により、前記第二のファイアウォール85から、前記第一のコネクションを介して前記サービス装置87から送信されてきたケットを受信した際に、そのケットに格納されている遠隔操作実行用のコマンドが正当なコマンドであるか否かを認証する。

【0056】したがって、顧客の内部ネットワーク82と遠隔操作サービス提供者の内部ネットワーク86

が、それぞれが接続されている外部ネットワーク84に対して互いに第一のファイアウォール83、第二のファイアウォール85を設置しているシステムにおいて、顧客及び遠隔操作サービス提供者がそれぞれの内部ネットワークのセキュリティの安全性を保持したまま、サービス装置87が顧客の被サービス装置81に対して、遠隔操作のサービスを実施することができる。

【0057】

【実施例】以下、図面を参照しながら、本発明の実施例を説明する。図5は、本発明の一実施例である遠隔保守及び遠隔操作を行うシステムの全体構成を示す図である。

【0058】同図において、自社ネットワーク110は、上記遠隔保守及び遠隔操作のサービスを実施する業者であるA社の社内ネットワークであり、顧客ネットワーク210は該サービスを受けるユーザであるD社の社内ネットワークである。

【0059】A社の自社ネットワーク110とD社の顧客ネットワーク210は、公衆回線または商用インターネットなどの回線250によって互いに接続されている。但し、A社の自社ネットワーク110と回線250の間にはファイアウォールとして機能する遠隔保守／操作センタ装置120が設置され、また、顧客ネットワーク210と回線250の間にはファイアウォール220が設置されている。

【0060】自社ネットワーク110には、遠隔保守及び遠隔操作のサービスを実行するサービス装置130が接続されている。また、顧客ネットワーク210には、該サービス装置130によって上記遠隔保守及び遠隔操作のサービスを受ける被サービス装置230が接続されている。

【0061】遠隔保守／操作センタ装置120は、自社ネットワーク110のサービス装置130に対して顧客ネットワーク210に接続された被サービス装置230にケット（IPデータグラム）の中継処理を提供する。また、自社ネットワーク110のセキュリティを保持するためにユーザ認証機能を備えている。このユーザ認証機能は、ユーザ認証用データベース121を備えることによって実現されている。

【0062】ユーザ認証用データベース121は、被サービス装置ID、ユーザID、パスワード、及びサービスIDの4種類の情報を、サービスを提供する各被サービス装置230毎に、個別に、記憶している。

【0063】また、遠隔保守／操作センタ装置120は、サービス装置データベース122も備えている。このサービス装置データベース122は、上記ユーザ認証用データベース121に登録されているサービスIDを有するサービス装置130のIPアドレスを記憶している。

【0064】また、さらに、遠隔保守／操作センタ装置

120は、被サービス装置被接続部124、サービス装置接続部125、及び自社ネットワーク安全保持部126を備えている。

【0065】被サービス装置被接続部124は、顧客ネットワーク210に接続されている被サービス装置230との間でファイアウォール220を介して、TCPプロトコルにより論理的なパスであるコネクション（コネクションA）を確立する。尚、この場合、該コネクションAの確立要求は、顧客ネットワーク210に接続された被サービス装置230側からなされる。被サービス装置被接続部124は、このコネクションAによって設定されたパスAを利用することにより、サービス装置130から送出される被サービス装置230宛のパケットをファイアウォール220を通過させ、顧客ネットワーク210を介して被サービス装置230に届けさせる。

【0066】サービス装置接続部125は、該被サービス装置被接続部124からの依頼を受けて、遠隔保守／操作センタ装置120とサービス装置130との間に、自社ネットワーク安全保持部126を介してTCPプロトコルにより論理的なパスであるコネクション（コネクションB）を確立させる。但し、このコネクションBの確立要求は、上記コネクションAが確立された後に、被サービス装置230が上記パスAにより送ってくるパケットのデータ部に含まれるサービスID、ユーザID、被サービス装置ID、及びパスワードによって、被サービス装置230が正しい契約ユーザの装置であると認識された後に、なされる。

【0067】自社ネットワーク安全保持部126は、該サービス装置被接続部124からの依頼を受けて、上述した被サービス装置230が契約ユーザであるかの認証処理を、前記ユーザ認証用データベース121を参照することにより実行する。そして、その認証結果を被サービス装置被接続部124に返す。

【0068】サービス装置130は、センタ被接続部132と遠隔保守／操作実行部134を備えている。センタ被接続部132は、自社ネットワーク110を介して遠隔保守／操作センタ装置120内のサービス装置接続部125との間で前記コネクションBを確立する。そして、該コネクションBによって設定されたパスBを介して、該サービス装置接続部125から被サービス装置230が送信してきた遠隔保守／操作要求のパケットを受け取る。そして、この要求を遠隔保守／操作実行部134に伝える。また、該遠隔保守／操作実行部134から依頼される遠隔保守／操作実行用のコマンドが格納されたパケットを、上記パスBを介して遠隔保守／操作センタ装置120内のサービス装置接続部125に送信する。

【0069】遠隔保守／操作実行部134は、該サービス装置接続部125から被サービス装置230が送信してきた遠隔保守／操作の開始要求依頼のメッセージが格

納されたパケットを受け取ると、被サービス装置230の遠隔保守／操作を実行するためのコマンドがデータ部に格納された該被サービス装置230宛のパケットを生成し、このパケットを遠隔保守／操作センタ装置120のサービス装置130に送信するようにセンタ被接続部132に依頼する。このパケットは、該センタ被接続部132により、コネクションBを介して遠隔保守／操作センタ装置120のサービス装置接続部125に送られ、さらに、被サービス装置被接続部124によりコネクションAを介して、被サービス装置230に送られる。遠隔保守／操作実行部134は、例えば、自社が顧客に販売した装置やソフトウェアなどの障害調査や障害の修正などを遠隔操作により実行する。

【0070】また、被サービス装置230は、センタ接続部232、遠隔保守／操作被実行部234、及び被サービス装置安全保持部235などから構成される。センタ接続部232は、自装置230の遠隔保守／操作を、契約先のサービス装置130に依頼する際に、自社のファイアウォール220を介して遠隔保守／操作センタ装置120の被サービス装置被接続部124との間にコネクションAを確立する。そして、以後、該コネクションAと前記コネクションBとで構成される二次パスを介して、サービス装置130との間で遠隔保守／操作を実施するためのコマンドや該遠隔保守／操作結果が格納されたパケットの授受を行う。

【0071】遠隔保守／操作被実行部234は、該センタ接続部232からサービス装置130から送信されてくるパケットを受取り、該パケットから遠隔保守／操作用のコマンドを取り出し、このコマンドを解析・実行する。そして、該コマンドの実行結果、すなわち、遠隔保守／操作の実行結果が格納されたパケットを生成し、このパケットをサービス装置130に送信してくれるように、センタ接続部232に依頼する。該センタ接続部232は、このパケットを上記コネクションAを介して遠隔保守／操作センタ装置120の被サービス装置被接続部124に送信する。

【0072】被サービス装置安全保持部235は、遠隔保守／操作被実行部234からの依頼を受けて、該遠隔保守／操作被実行部234がサービス装置130から受け取ったパケットのセキュリティ・チェックを行う。すなわち、そのパケットに格納されているコマンドが契約で定められた正当なコマンドであるか否かなどをチェックする。そして、そのチェック結果を遠隔保守／操作被実行部234に返す。このセキュリティ・チェックは、例えば、サービス提供者がアクセスしてほしくないファイルを保護するために行われる。

【0073】被サービス装置230は、該被サービス装置安全保持部235が上記セキュリティ・チェックを行うためのデータベースとして、非参照ファイル名データベース236を備えている。

10

20

30

40

50

【0074】この非参照ファイル名データベース236には、顧客がサービス装置130に対してアクセスを禁止するファイルの名称が登録されている。上記被サービス装置安全保持部235は、サービス装置130から送られてくるパケットに格納されているコマンドがこれらのアクセス保護対象のファイルであった場合には、そのコマンドの実行を禁止するように遠隔保守／操作実行部134に通知する。

【0075】これにより、遠隔保守／操作被実行部234は、サービス装置130から指示されるコマンドの内、自社のセキュリティの安全が保持されるコマンドのみを実行する。

【0076】次に、上記構成の実施例での動作を、図6を参照しながら説明する。本実施例では、遠隔保守／操作の実行は、顧客側からの要求によって開始される。この要求は、例えば、被サービス装置230の表示部に表示されるGUI（グラフィカル・ユーザ・インターフェース）を介して指示される（S11）。

【0077】この指示がなされると、センタ接続部232は、顧客ネットワーク210及びファイアウォール220を介して、遠隔保守／操作センタ装置120の被サービス装置被接続部124とコネクションAを確立する。これにより、センタ接続部232と被サービス装置被接続部124との間にセッションが開設され、これら両部232、124がコネクションAを介してパケットを授受することが可能になる。

【0078】続いて、センタ接続部232は、契約時に被サービス装置230に割当てられたサービスID、ユーザID、被サービス装置ID、及びパスワードが格納されたパケットを生成し、このパケットを上記コネクションAを介して、遠隔保守／操作センタ装置120の被サービス装置被接続部124に送信する（S12）。

【0079】被サービス装置被接続部124は、上記パケットを受信すると、該パケットに格納されているサービスID、ユーザID、被サービス装置ID、及びパスワードを自社ネットワーク安全保持部126に送り、上記パケットが契約ユーザの被サービス装置被接続部124から送られてきたものかの判断を依頼する。該自社ネットワーク安全保持部126は、上記4種類の情報をユーザ認証用データベース121に登録されている情報と照合し、上記パケットが契約ユーザからのものであるかを判定する。そして、契約ユーザからのパケットであると判定すると（S14）、上記サービスIDをキーとしてサービス装置データベース122を検索して、該サービスIDに対応するサービス装置130を識別し、そのサービス装置130のIPアドレスを獲得する。そして、該照合結果と共に契約ユーザからのパケットであることが判明した場合には、上記識別したサービス装置130のIPアドレスも被サービス装置被接続部124に返す（S15）。

【0080】一方、上記ステップS14で上記パケットが契約ユーザからのものでないと判断した場合には、このパケットを棄却する。また、上記コネクションAを切断する。

【0081】該被サービス装置被接続部124は、自社ネットワーク安全保持部126から上記判定結果を受け取り、自己が受信したパケットが契約ユーザの被サービス装置230から送信されてきたものであると判断すると、上記識別された自社ネットワーク安全保持部126に接続されたサービス装置130のIPアドレスをサービス装置接続部125に送り、該サービス装置130との間にコネクションBを確立するように依頼する。サービス装置接続部125は、この依頼を受けて、自社ネットワーク110を介して上記コネクションBを、上記サービス装置130のセンタ接続部232との間に確立する（S16）。

【0082】これにより、サービス装置接続部125とセンタ接続部232との間にセッションが開設され、これら両部125、232は、互いにパケットを授受することが可能になる。尚、自社ネットワーク安全保持部126が、サービス装置接続部125に、直接、上記コネクションBの確立を依頼するようにしてもよい。

【0083】続いて、サービス装置接続部125は、上記コネクションBを介して、上記サービス装置130のセンタ接続部232に被サービス装置230との間でパケット通信が可能になったことを通知する（S17）。

【0084】該センタ接続部232は、この通知を受けて、遠隔保守／操作実行部134に被サービス装置230に対する遠隔保守／操作の実行を開始するように要求する。遠隔保守／操作実行部134は、この要求を受け取ると、予め、契約時に定められた遠隔保守／操作の実施を開始する。この実施は、該遠隔保守／操作実行用のコマンドが格納されたパケットを契約先の被サービス装置230に送信することによって実行される。すなわち、遠隔保守／操作実行部134は、このパケットを生成し、これを上記被サービス装置230に送信してくれるようにセンタ被接続部132センタに依頼する（S18）。

【0085】該センタ被接続部132は、上記依頼を受けると、該遠隔保守／操作実行用のパケットを、コネクションBを介して遠隔保守／操作センタ装置120のサービス装置接続部125に送信する（S19）。

【0086】該サービス装置接続部125は、上記遠隔保守／操作実行用のパケットを受け取ると、このパケットをコネクションAを介して被サービス装置230のセンタ被接続部132に送信する（S20）。

【0087】該センタ被接続部132は、上記遠隔保守／操作実行用のパケットを受信すると、このパケットの正当性のチェックを被サービス装置安全保持部235に依頼する。そして、被サービス装置安全保持部235が

ら、該パケットに格納されている遠隔保守／操作実行用のコマンドが正しいものであるとの判定結果を受け取ると、該コマンドの実行を遠隔保守／操作実行部134に依頼する。該遠隔保守／操作実行部134は、該コマンドを実行し、その実行結果が格納されたパケットを生成し、このパケットをサービス装置130に送信してくれるように、センタ被接続部132に依頼する。該センタ被接続部132は、受け取ったパケットをコネクションAを介して遠隔保守／操作センタ装置120の被サービス装置被接続部124に送信する(S21)。

【0088】尚、このとき、被サービス装置安全保持部235によって、上記サービス装置130が指示するコマンドが非参照ファイル名データベース236に登録されているファイルをアクセスするコマンドであると判定されたならば、遠隔保守／操作実行部134は該コマンドを実行しない(S22)。

【0089】該被サービス装置被接続部124は、該遠隔保守／操作の実行結果が格納されたパケットを受信すると、このパケットをコネクションBを介してサービス装置130のセンタ被接続部132に送信する(S23)。

【0090】該センタ被接続部132は、上記パケットを受信すると、該パケットから上記遠隔保守／操作の実行結果を取り出し、これを遠隔保守／操作実行部134に送る。該遠隔保守／操作実行部134は、該実行結果を自装置130の表示部に画面表示する(S24)。

【0091】上記ステップS18～S24の処理は、被サービス装置230で遠隔保守／操作の実行が指示される間、繰り返される。尚、この遠隔保守／操作の実行指示は、例えば、サービス装置130の表示の画面に表示されるGUI(グラフィカル・ユーザ・インターフェイス)を介しておこなわれる。

【0092】遠隔保守／操作実行部134は、被サービス装置230に対する全ての遠隔保守／操作の実行を終了すると、センタ被接続部132に遠隔保守／操作の実施が終了した旨をセンタ被接続部132に通知する(S25)。

【0093】該センタ被接続部132は、この通知を受けて上記コネクションBの切断処理を実行する(S26)。遠隔保守／操作センタ装置120のサービス装置被接続部125は、上記コネクションBの切断処理が終了すると、新しいパスワードを被サービス装置230に送付するためのパケットを生成し、このパケットをコネクションAを介して、被サービス装置230のセンタ被接続部132に送信する。遠隔保守／操作センタ装置120の被サービス装置被接続部124は、被サービス装置230からその新しいパスワードの受信の確認を受け取ると、コネクションAを切断する処理を行う(S27)。

【0094】被サービス装置230は、上記コネクシ

ンAの切断処理が終了した後、この新しいパスワードを、次の遠隔保守／操作のために使用するために所定の記憶装置に記憶する(S28)。

【0095】次に、上記遠隔保守／操作の実行時におけるパケットの流れを、詳細に説明する。ここでは、図7に示すように自社ネットワーク110と顧客ネットワーク210が互いにインターネット250によって接続され、自社ネットワーク110内の遠隔保守／操作センタ装置120とサービス装置130、及び顧客ネットワーク210のファイアウォール220と被サービス装置230に対して、同図に示すようなIPアドレスとポート番号が割り当てられているものとして説明する。

【0096】すなわち、自社ネットワーク110においては、遠隔保守／操作センタ装置120のIPアドレスは”C”に、その被サービス装置被接続部124のポート番号は”P1”に設定されている。また、サービス装置130のIPアドレスは、”D”に設定されている。

【0097】一方、顧客ネットワーク210においては、被サービス装置230のIPアドレスは”A”に、そのセンタ被接続部132のポート番号は”P2”に設定されている。また、ファイアウォール220のIPアドレスは”B”に設定されている。

【0098】次に、図8は、自社ネットワーク110と顧客ネットワーク210間で授受されるパケット内のIPデータグラムに設定されるヘッダ部300の構成を示す図である。

【0099】上記ヘッダ部300は、IPヘッダ301とTCPヘッダ302に加え、遠隔保守／操作ヘッダとから構成される。IPヘッダ301には、発信IPアドレス(ソースアドレス)、受信IPアドレス(デスティネーションアドレス)などIPプロトコルによって定められている各種情報が設定される。また、TCPヘッダ302には、発信ポート番号(ソースポート番号)、受信ポート番号(デスティネーションポート番号)、SEQ(Sequence Number)などTCPプロトコルによって定められている各種情報が設定される。

【0100】また、遠隔保守／操作ヘッダ303は、本実施例の特徴となるもので、前述したように、被サービス装置被接続部124がコネクションAを介して受信するパケットが、契約先のユーザからのものであるか否かを判定するためのセキュリティ・チェックに用いられるサービスID(SVID)、ユーザID(UID)、パスワード(PWD)、及び被サービス装置ID(WID)が設定される。この遠隔保守／操作ヘッダ303は、上記TCPヘッダ302のデータ部に設定される。

【0101】図9～図11は、図6のフローチャートで説明した処理におけるパケットの流れとそのパケットの内容を説明する図である。ここで、図12に、被サービス装置230とサービス装置130間で送受信されるパケット400のフォーマットを示す。このパケット40

0は、通常のIPデータグラムのTCP/IPヘッダ400aの後に、上記被サービス装置230とサービス装置130との間で遠隔保守／操作を実施するために用いる遠隔保守／操作ヘッダ400bと通知情報などのデータ400cが設定される。上記TCP/IPヘッダ400aは、前記図8に示すIPヘッダ301とTCPヘッダ302とから構成され、また、上記遠隔保守／操作ヘッダ400bの内容は、図8に示す遠隔保守／操作ヘッダ303のようになっている。

【0102】また、図9～図11に示すパケット401～406の内、被サービス装置230からサービス装置130に送信されるパケット401～403のTCP/IPヘッダの形式は図13(a)に示す通りである。また、サービス装置130から被サービス装置230に送信されるパケット404～406のTCP/IPヘッダの形式は図13(b)に示す通りである。

【0103】図9から図11に示す被サービス装置230とサービス装置130との間でのパケット(IPデータグラム)の通信では、被サービス装置230と遠隔保守／操作センタ装置120間に確立されるコネクション(セッション)Aと遠隔保守／操作センタ装置120とサービス装置130間に確立されるコネクション(セッション)Bが利用される。

【0104】顧客ネットワーク210の被サービス装置230のセンタ接続部232は、コネクションAを確立した後、図13に示すTCPヘッダのデータ部に遠隔保守／操作ヘッダが格納されたパケット(IPデータグラム)401をファイアウォール220に送信する。該ファイアウォール220は、このパケット401を顧客ネットワーク210を介して受信すると、IPヘッダの発信IPアドレスを、被サービス装置230のIPアドレスである“A”から自己のIPアドレスである“B”に置き換える。そして、この発信IPアドレスの置き換えが行われたパケット(IPデータグラム)402をインターネット250を介して顧客ネットワーク210の遠隔保守／操作センタ装置120の被サービス装置被接続部124に送信する。

【0105】以上のパケットの通信はコネクション(セッション)Aを用いて行われる。このとき、自社ネットワーク110の遠隔保守／操作センタ装置120が受信するパケット402の発信IPアドレスには、顧客ネットワーク210に設置されたファイアウォール220のIPアドレス“B”が設定されているので、自社ネットワーク110は、被サービス装置230のIPアドレス“A”を知ることはできない。

【0106】遠隔保守／操作センタ装置120は、上記パケット402を受信すると顧客ネットワーク210側のファイアウォール220とのセッションAを維持したまま、該パケット402の遠隔保守／操作ヘッダを調べる。すなわち、自社ネットワーク安全保持部126が、

該遠隔保守／操作ヘッダに設定されている、サービスID、ユーザID、パスワード、及び被サービス装置IDがユーザ認証用データベース121に登録されているか否か調べる。そして、該登録が確認されたならば、上記サービスIDを基に、サービス装置データベース122からそのサービスIDを有するサービス装置130のIPアドレス(この場合、“D”)を取り出す。サービス装置接続部125は、このIPアドレス“D”を自社ネットワーク安全保持部126から受け取り、サービス装置130のセンタ被接続部132との間にコネクション(セッション)Bを確立する。

【0107】続いて、センタ被接続部132は、図10に示すパケット(IPデータグラム)403を生成する。すなわち、該パケット403の受信IPアドレスに“D”を設定すると共に、発信IPアドレスに自己のIPアドレス“C”を設定する。また、このパケット403の受信ポート番号にサービス装置130のセンタ接続部232に割り当てられるポート番号(この場合、“P3”)を設定する。また、TCPヘッダのデータ部分に、ユーザからのセッション要求の通知情報を設定する。そして、サービス装置接続部125は、このパケット403を自社ネットワーク110を介してサービス装置130のセンタ被接続部132に送信する。

【0108】サービス装置130では、上記パケット403をセンタ被接続部132により受信すると、遠隔保守／操作実行部134が該パケット403のデータ部に格納されているユーザ(サービス提供者)からの指示データを解釈する。そして、該指示データによって指示されている保守／操作を実行するためのコマンド(サービス提供者への指示情報)を作成し、このコマンドがデータ部にセットされたパケット(IPデータグラム)404を生成する。また、この場合、パケット404の受信IPアドレスに遠隔保守／操作センタ装置120のIPアドレス“A”を、送信IPアドレスにサービス装置130のIPアドレス“D”を設定する。さらに、受信ポート番号に遠隔保守／操作センタ装置120のサービス装置接続部125のポート番号“P3”を、送信ポート番号にセンタ被接続部132のポート番号“P3”を設定する。そして、センタ被接続部132は、このパケット404をコネクションBを介して遠隔保守／操作センタ装置120のサービス装置接続部125に送信する。

【0109】遠隔保守／操作センタ装置120の被サービス装置被接続部124は、このパケット404をサービス装置接続部125から受け取ると、図10に示すパケット(IPデータグラム)405を生成する。サービス装置接続部125は、パケット404の受信IPアドレス、発信IPアドレス、及び受信ポート番号を変換する。すなわち、パケット405の受信IPアドレスに顧客ネットワーク210のファイアウォール220のIPアドレス“B”を、発信IPアドレスに自装置120の

IPアドレス”C”を設定する。さらに、受信ポート番号に顧客ネットワーク210に接続された被サービス装置230のセンタ被接続部132のポート番号”P2”を設定する。そして、被サービス装置被接続部124は、コネクションAを介してこのパケット405を顧客ネットワーク210のファイアウォール220に送信する。ファイアウォール220は、該パケット405を受信すると、まず、IPアドレスの変換処理を行い、図11に示すパケット（IPデータグラム）406を生成する。すなわち、受信IPアドレスを”B”から被サービス装置230のIPアドレス”A”に、発信IPアドレスを”C”から自己のIPアドレス”B”に変換する。そして、ファイアウォール220は、被サービス装置230からのセッションを利用してパケット406を被サービス装置230のセンタ接続部232に送信する。

【0110】このように、被サービス装置230は、発信IPアドレスがファイアウォール220のIPアドレスのパケットのみを受信する。したがって、サービス装置130のIPアドレスを知ることはできない。

【0111】センタ接続部232は、該パケット406を受信すると、これを遠隔保守／操作実行部134に送る。遠隔保守／操作実行部134は、該パケット406からサービス提供者の指示情報を取り出し、これを解釈して、その指示情報によって指示されている保守／操作を実行する。尚、この保守／操作の実行の前に被サービス装置安全保持部235によって、上記サービス提供者の指示情報が正当であるか否かのチェックが行われる。そして、遠隔保守／操作実行部134は、このチェックにより正当であると判定された指示情報のみを実行する。

【0112】遠隔保守／操作実行部134は、上記遠隔保守／操作の実行が終了すると、その実行結果がTCPヘッダのデータ部に格納されたパケット（IPデータグラム）を生成する。このパケットは、以上、説明した、コネクションA及びコネクションBにより結ばれた二次パス（図5参照）を逆方向に經由して、自社ネットワーク110に接続されたサービス装置130に送られる。

【0113】次に、遠隔保守／操作センタ装置120が、顧客ネットワーク210に設置されたファイアウォール220を介して、該顧客ネットワーク210に接続された被サービス装置230とコネクション（セッション）Aを確立する動作を、より詳細に説明する。

【0114】図14は、遠隔保守／操作センタ装置120が被サービス装置230とサービス装置130との間のパケット（IPデータグラム）の中継処理を実行する動作を説明するフローチャートである。遠隔保守／操作センタ装置120が被サービス装置230とサービス装置130との間のパケット（IPデータグラム）の中継処理を実行する動作を説明するフローチャートである。

【0115】ところで、顧客ネットワーク210に設置されたファイアウォール220は、例えば、TCPポートフィルタリング機能を備えており、遠隔保守／操作の契約が成立すると、遠隔保守／操作を提供する業者は、遠隔保守／操作センタ装置120の被サービス装置被接続部124に割当てられているポート番号を、契約先のユーザに通知する。これを受けて、契約先のファイアウォール220の管理者は、顧客ネットワーク210に接続された自社の被サービス装置230と遠隔保守／操作センタ装置120の被サービス装置被接続部124が互いにパケットをファイアウォール220を介して送受信できるように、ファイアウォール220のTCPポートフィルタリングを設定する。尚、上記被サービス装置被接続部124のポート番号は、固定であってもよく、また、各被サービス装置230ごとに個別のポート番号を割当ててもよい。

【0116】また、顧客ネットワーク210に設置されたファイアウォール220がIPアドレスフィルタリング機能を備えている場合には、遠隔保守／操作を提供する業者は、遠隔保守／操作センタ装置120のIPアドレスを契約先のユーザに知らせ、該遠隔保守／操作センタ装置120が被サービス装置230宛に送信するパケットがファイアウォール220を通過できるようにIPアドレスフィルタを設定してもらうようにお願いする。

【0117】被サービス装置被接続部124は、常時、被サービス装置230からのセッション（コネクション）確立要求待ちにある（S41）。そして、被サービス装置被接続部124は、ファイアウォール220を介して被サービス装置230が送信してきたセッション確立要求のメッセージが格納されたパケットを受け取ると、そのパケットの遠隔保守／操作ヘッダに設定されているサービスID、ユーザID、パスワード、及び被サービス装置IDがユーザ認証用データベース121に登録されているか否かのチェックを、自社ネットワーク安全保持部126に依頼する（S42）。

【0118】続いて、被サービス装置被接続部124は、自社ネットワーク安全保持部126からそのチェック結果を受取り、被サービス装置230が契約されたユーザのものであるか否かを判別する（S43）。

【0119】次に、被サービス装置被接続部124は、上記チェック結果により、セッション確立要求のパケットが契約先の被サービス装置230からのものでないと判別すると（S43、NG）、このセッション（コネクション）確立要求を棄却（リジェクト）する（S44）。

【0120】一方、被サービス装置被接続部124は、セッション確立要求のパケットが契約先の被サービス装置230からのものであると判別すると（S43、OK）、サービス装置被接続部125に上記パケットに格納されているサービスIDを送る。サービス装置被接続部1

25は、このサービスIDを受け取ると、このサービスIDに対応するサービス装置130のIPアドレスを、サービス装置データベース122を検索して、読み出す(S45)。

【0121】そして、サービス装置接続部125は、このIPアドレスを用いて、自社ネットワーク110を介して該IPアドレスを有するサービス装置130とセッション(コネクション)Bを確立する(S46)。

【0122】次に、サービス装置接続部125は、被サービス装置230とサービス装置130とのセッション(コネクション)を維持したままで、この新たにセッションが確立された被サービス装置230用の子プロセスを生成する(S47)。

【0123】続いて、サービス装置接続部125は、別の被サービス装置230からのセッション要求を待つシステム・コールを行い(S48)、上記ステップS41に戻る。

【0124】以上述べたステップS41～S48の処理により、遠隔保守/操作センタ装置120により、被サービス装置230とサービス装置130との間には複数のセッションが確立される。すなわち、サービス装置130は複数の被サービス装置230に対して遠隔保守/操作のサービスを実施することができる。

【0125】図14には、被サービス装置A、B、及びCの3台の被サービス装置230とサービス装置130との間に確立されたセッションによって生成された子プロセスが示されている。各子プロセスは、被サービス装置230用のバッファ127(127A、127B、127C)とサービス装置130用のバッファ128(128A、128B、128C)を備える。被サービス装置230からサービス装置130に対してパケットが送信される場合には、このパケットは、いったん被サービス装置被接続部124によって被サービス装置230用のバッファ127に格納された後、該バッファ127からサービス装置130用のバッファ128にコピーされる。そして、このバッファ128に格納されたパケットは、サービス装置接続部125によって取り出され、該サービス装置接続部125によって当該サービス装置130に送出される。

【0126】また、図14には示していないが、サービス装置130から被サービス装置230に対してパケットが送信される場合には、このパケットは、いったんサービス装置被接続部125によってサービス装置130用のバッファ128に格納された後、該バッファ128から被サービス装置230用のバッファ127にコピーされる。そして、このバッファ127に格納されたパケットは、被サービス装置被接続部124によって取り出され、該被サービス装置被接続部124によって当該被サービス装置230に送出される。

【0127】以上のようにして、コネクションAとコネ

クションBの2つのコネクションを用いることにより、遠隔保守/操作センタ装置120を介して、被サービス装置230とサービス装置130との間でパケット(IPデータグラム)の授受が行われ、該サービス装置130によって、該被サービス装置230の遠隔保守/操作が実施される。

【0128】次に、図15は、遠隔保守/操作センタ装置120のIP中継機能を別の観点から説明するフローチャートである。同図において、前記図14で説明したステップと同一のステップS41～S46によって、被サービス装置230からのセッション確立要求によって、サービス装置接続部125が自社ネットワーク110を介してサービス装置130との間にセッション(コネクションB)を確立する。

【0129】該サービス装置接続部125は、上記セッションを確立すると、セッション管理テーブルを作成する(S51)。このセッション管理テーブルは、(セッション番号、被サービス装置セッションID、サービス装置セッションID)の3種類の情報から成る。被サービス装置セッションIDは、被サービス装置230と被サービス装置被接続部124との間に確立されるコネクションAによって開設されるセッションに関するものである。また、サービス装置セッションIDは、サービス装置接続部125と被サービス装置230との間に確立されるコネクションBによって開設されるセッションに関するものである。この被サービス装置セッションIDとサービス装置セッションIDによって、被サービス装置230とサービス装置130との間に確立される一本の論理パスに関する情報が得られ、遠隔保守/操作センタ装置120は、被サービス装置230とサービス装置130との間で授受されるパケット(IPデータグラム)の中継処理を実行できる。尚、上記セッションIDは、サービス装置接続部125がTCPプロトコル層で管理しているもので、発信IPアドレス、受信IPアドレス、発信ポート番号、受信ポート番号などの情報により区別される各個別のセッション(コネクション)を識別するためのIDである。セッション管理テーブルにおいては、一組の被サービス装置セッションIDとサービス装置セッションIDによって定まる被サービス装置230とサービス装置130との間の各セッションについて、一意のセッション番号が割当てられる。

【0130】続いて、遠隔保守/操作センタ装置120(被サービス装置被接続部124またはサービス装置被接続部125)は、各装置(被サービス装置230またはサービス装置130)から送信されてくるパケットの入力待ちとなる(S52)。

【0131】そして、遠隔保守/操作センタ装置120(被サービス装置被接続部124またはサービス装置被接続部125)は、各装置(被サービス装置230またはサービス装置130)からパケットを入力すると、前記

セッション管理テーブルを検索して、上記入力されたパケットが送信されてきたセッションのID（セッションID）を基に、セッション管理テーブルを検索して（S53）、該セッション管理テーブルから上記セッションIDに対応する装置（被サービス装置230またはサービス装置130）のセッションIDを取り出す（S54）。すなわち、被サービス装置230からのパケットを被サービス装置被接続部124が受信した場合には、該被サービス装置被接続部124は、そのパケットが送られてきたセッション（被サービス装置セッションID）に対応するサービス装置セッションIDを取り出す。一方、サービス装置130からのパケットをサービス装置接続部125が受信した場合には、該サービス装置接続部125は、そのパケットが送られてきたセッション（サービス装置セッションID）に対応する被サービス装置230サービス装置セッションIDを取り出す。

【0132】そして、サービス装置接続部125は、上記取り出したセッションIDを基に、被サービス装置230から送信されてきたパケットを、当該サービス装置130に送出する。また、被サービス装置被接続部124は、上記取り出したセッションIDを基に、サービス装置130から送信されてきたパケットを、当該被サービス装置230に送出する（S55）。

【0133】以上、述べたように、本実施例によれば、遠隔保守／操作サービスを提供する業者の内部ネットワークと該業者から遠隔保守／操作のサービスを受ける装置を有する顧客のネットワークが、インターネットや公衆回線などの外部ネットワークによって互いに接続され、かつ、両社が該外部ネットワークに対してファイアウォールを設置しているシステム形態において、遠隔保守／操作サービス提供業者は内部ネットワークに接続されているサービス装置を用いて、顧客側の内部ネットワークに接続されている被サービス装置を、遠隔保守／操作することができる。しかも、この場合、互いにセキュリティ・ガード機構を備えているので、両者とも内部ネットワークの安全性を保持することができる。

【0134】また、本実施例では、上記外部ネットワークとして商用インターネットを利用することが可能である。この場合、ダイヤル・アップIP接続のユーザも顧客の対象にすることができる。また、この場合、商用インターネットとの回線接続時にIPアドレスが割当てられる端末型のダイヤル・アップIP接続を利用するユーザも顧客の対象にすることができる。すなわち、本実施例では、受信したパケットが契約先のユーザからのものであるか否かを、契約時に登録されるサービスID、ユーザID、被サービス装置ID、及びパスワードにより認証するので、IPアドレスのみに頼らずに、契約ユーザの認証を行うことが可能だからである。

【0135】尚、上記実施例では、TCP/IPプロト

コルを利用して遠隔保守／操作を実施するためのパケットの送受信を行うようにしているが、本発明は、プロトコルが限定されるものではなく、その他のプロトコルを採用することも可能である。また、契約先のユーザと遠隔保守／操作の提供業者のそれぞれの社内ネットワークは、必ずしも、インターネットで接続されている必要はなく、その他のコモン・キャリアによって提供される各種のネットワークで接続されていてもよい。また、遠隔保守／操作のみならず、広い意味での遠隔操作全般に適用可能なものである。

【0136】

【発明の効果】本発明によれば、遠隔操作サービスを受ける顧客と該サービスを実施する業者が、外部ネットワークにファイアウォールを設置したままで、それぞれの社内ネットワークに接続された装置により、遠隔操作を実施できる。したがって、既存の社内ネットワークをそのまま利用して、安全で安価な遠隔操作サービスシステムを実現できる。

【0137】また、被サービス装置には、契約事項以外の遠隔操作の実行を阻止するセキュリティ・チェック機構が設けられるので、安全性は保証される。一方、遠隔操作実施業者でも、契約ユーザの被サービス装置とコネクションを確立した後に、該コネクションを介して送られてくるパケットに正式な契約ユーザであることを示す認証情報が設定されているか否かをチェックするセキュリティ・チェック機構を設けているので、サービス装置に対する不正なアクセスを防止できる。

【図面の簡単な説明】

【図1】本発明の原理を説明する図（その1）である。

【図2】本発明の原理を説明する図（その2）である。

【図3】本発明の原理を説明する図（その3）である。

【図4】本発明の原理を説明する図（その4）である。

【図5】本発明の一実施例である遠隔保守及び遠隔操作を行うシステムの全体構成を示す図である。

【図6】上記実施例の全体動作を説明する図である。

【図7】上記実施例の一つのシステム形態例を示す図である。

【図8】図7に示すシステムにおいて、自社ネットワークと顧客ネットワーク間で授受されるパケット内のIPデータグラムに設定されるヘッダ部の構成を示す図である。

【図9】図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、上記両装置間で授受されるパケットの内容を示す図（その1）である。

【図10】図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、上記両装置間で授受されるパケットの内容を示す図（その2）である。

【図11】図7に示すシステムでサービス装置が顧客の

被サービス装置の遠隔保守／操作を実施する際に、上記両装置間で授受されるパケットの内容を示す図（その3）である。

【図12】上記図9～図11に示す動作中において、被サービス装置とサービス装置間で送受信されるパケットのフォーマットを示す図である。

【図13】上記図9及び図11に示されたパケットのフォーマットを説明する図である。

【図14】遠隔保守／操作センタ装置が被サービス装置とサービス装置との間のパケット（IPデータグラム）の中継処理を実行する動作を説明するフローチャートである。

【図15】上記図14のフローチャートに示された遠隔保守／操作センタ装置120のIP中継機能を別の観点から説明するフローチャートである。

【図16】ファイアウォールのパケットフィルタリングゲートウェイ機能を説明する図である。

【図17】ファイアウォールの第二の機能であるIPアドレス変換／中継機能を説明する図である。

【図18】A社、B社、C社、及びD社の内部ネットワークがファイアウォールを介して、商用インターネットに接続されたシステムを示す図である。

【図19】上記図18に示すシステムにおいて、A社の内部ネットワークに接続されたサービス装置がD社の内部ネットワークに接続された被サービス装置の遠隔保守／操作を実施できない原因を説明する図である。

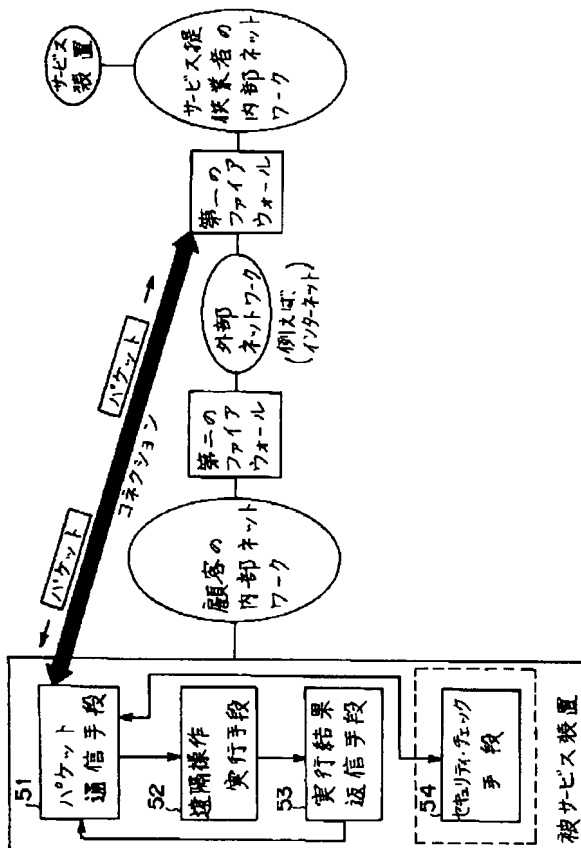
【図20】上記図18に示すシステムにおいて、A社の内部ネットワークに接続されたサービス装置がD社の内部ネットワークに接続された被サービス装置を遠隔保守／操作を実施する従来方法を説明する図である。

【符号の説明】

- 51、71 パケット通信手段
- 52、72 遠隔操作実行手段
- 53 実行結果返信手段
- 54、62 セキュリティ・チェック手段
- 61 第一のパケット通信手段
- 63 第二のパケット通信手段
- 81 被サービス装置
- 82 顧客の内部ネットワーク
- 83 第一のファイアウォール
- 84 外部ネットワーク
- 85 第二のファイアウォール
- 86 サービス提供者の内部ネットワーク
- 87 サービス装置

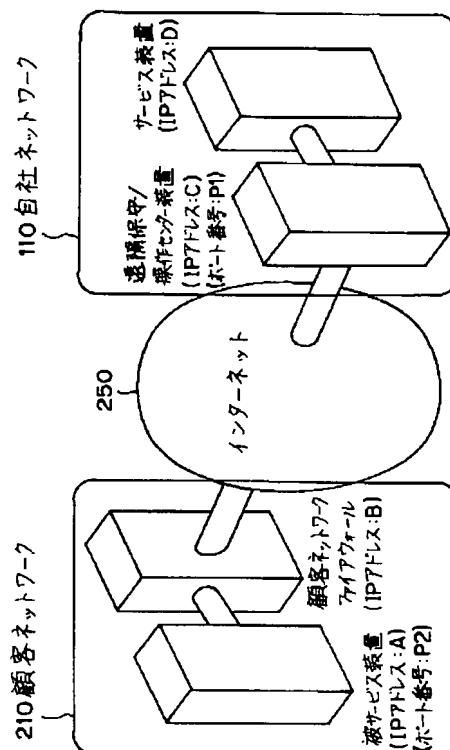
【図1】

本発明の原理を説明する図（その1）



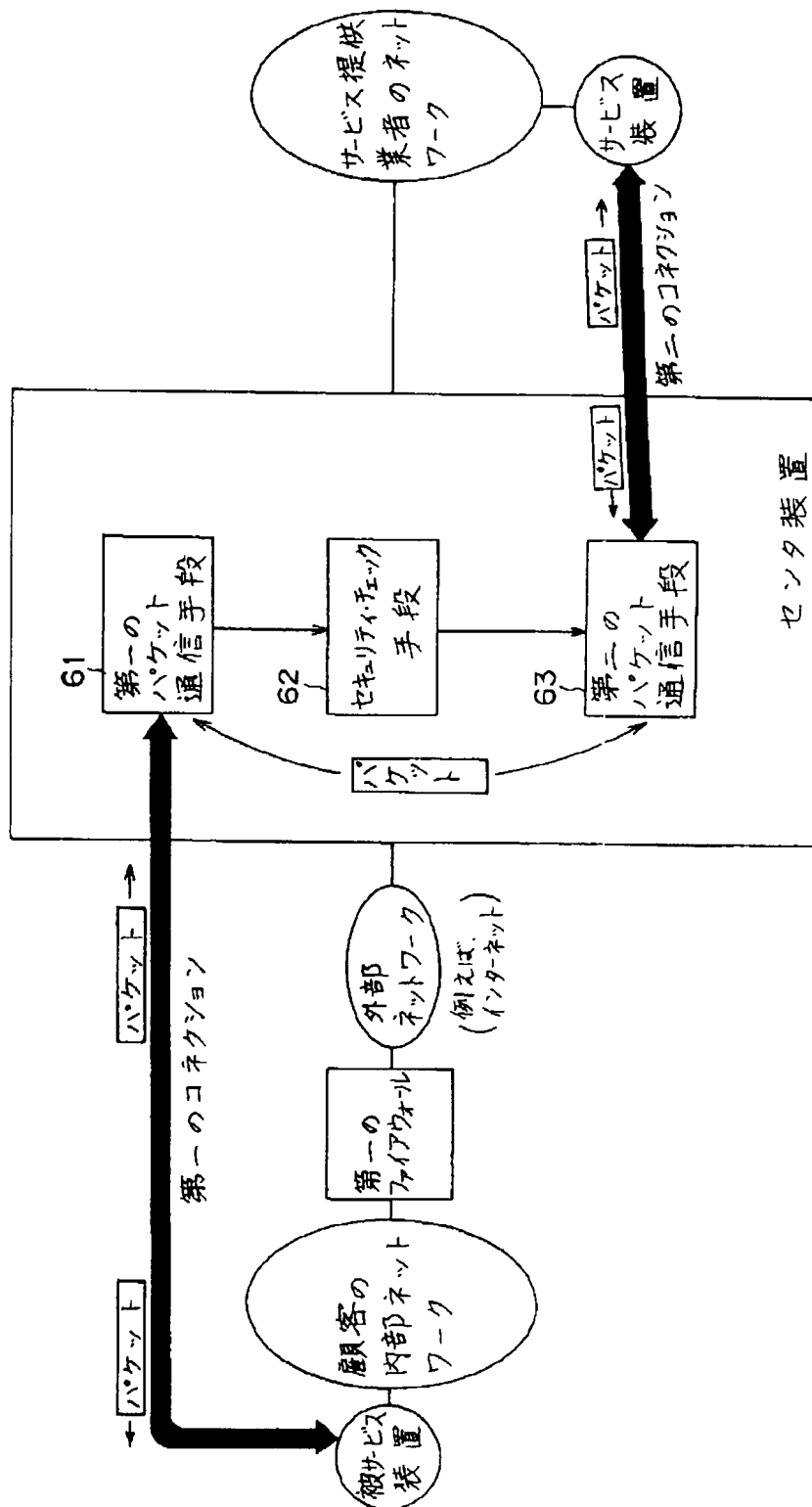
【図7】

実施例の一つのシステム形態例を示す図



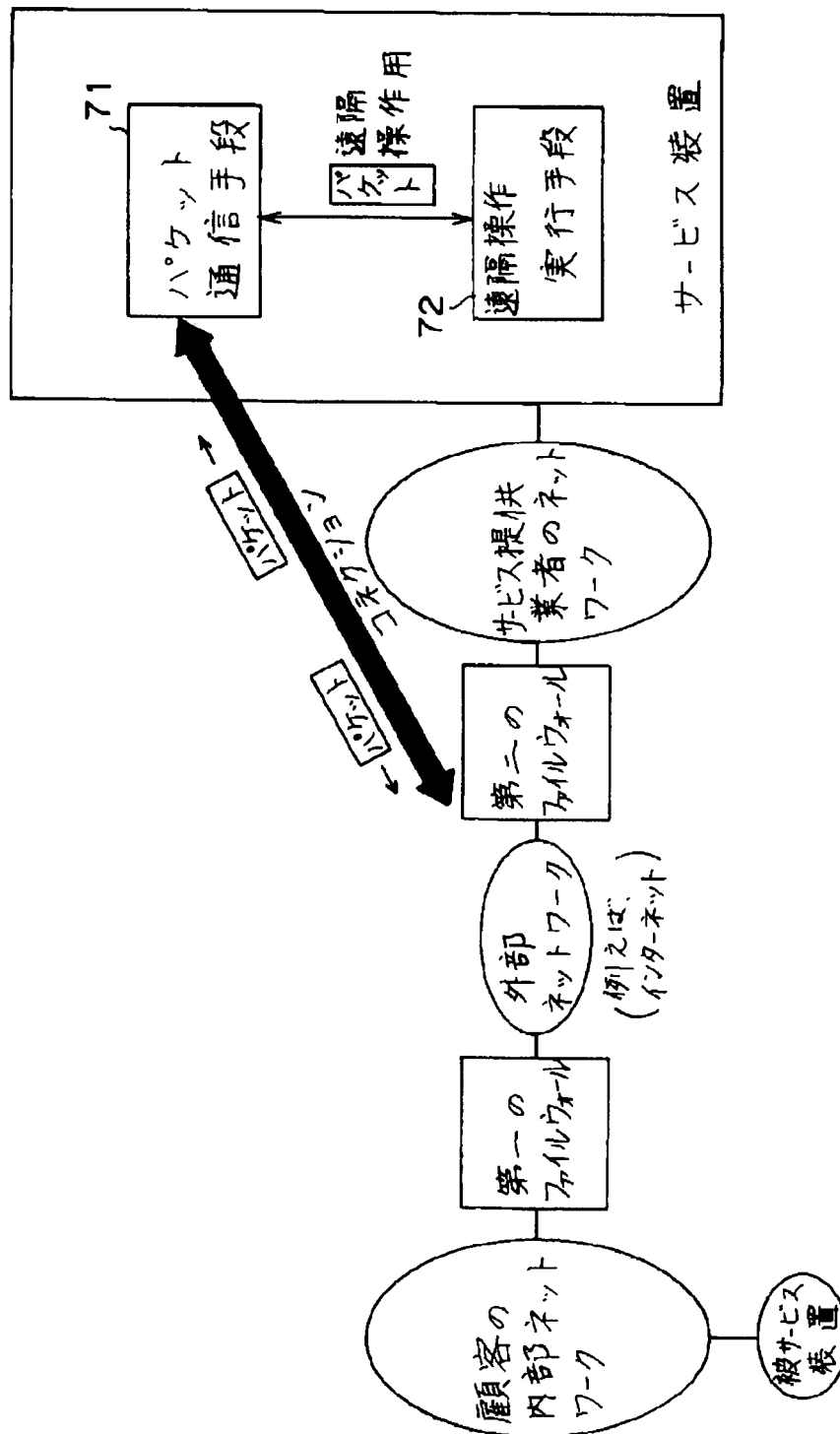
【図2】

本発明の原理を説明する図(その2)



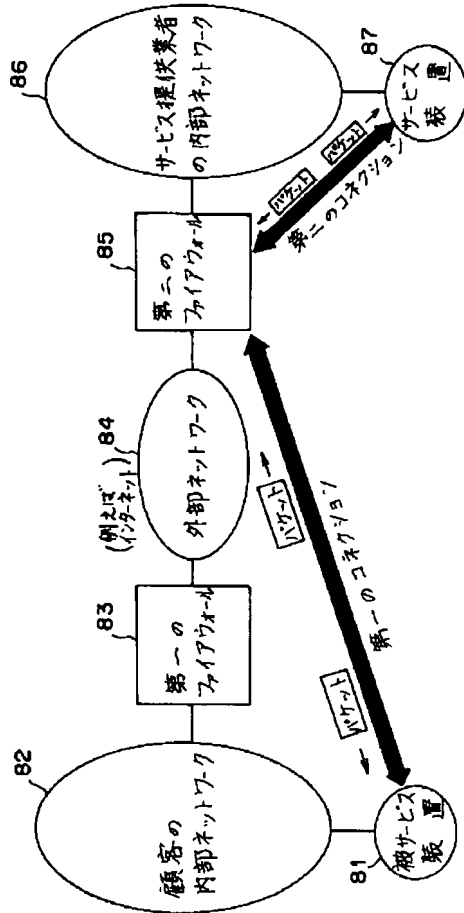
【図3】

本発明の原理を説明する図(その3)



【図4】

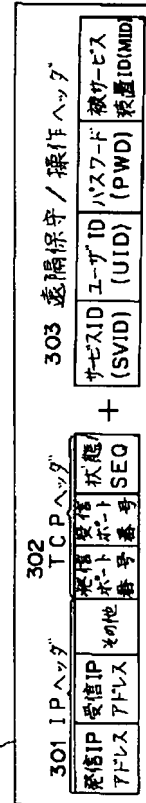
本発明の原理を説明する図（その4）



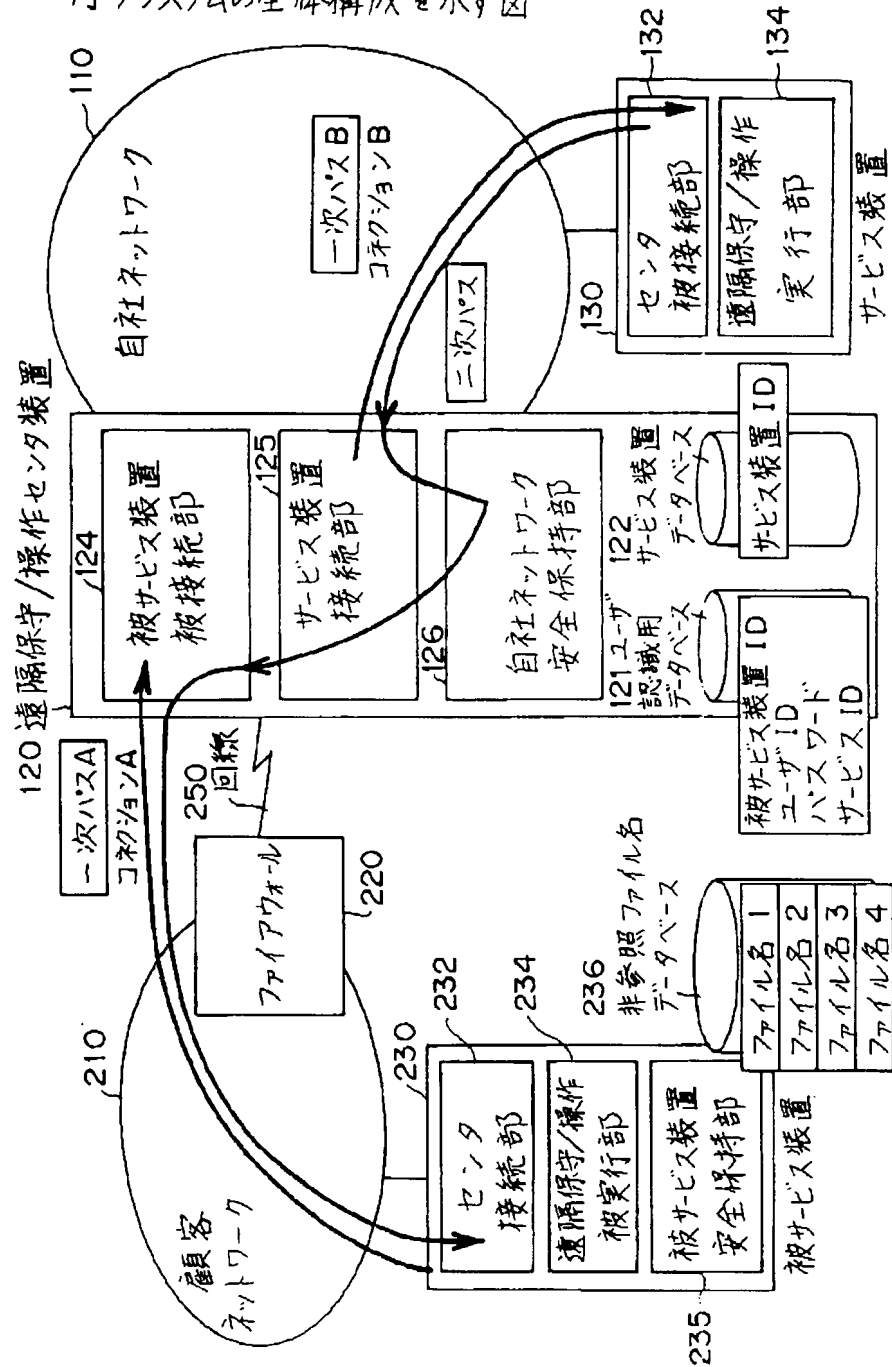
【図8】

図7に示すシステムにおいて、自社ネットワークと顧客ネットワーク間で授受されるパケット内のIPデータグラムに設定されるベッタ部の構成を示す図

パケットのヘッダ部

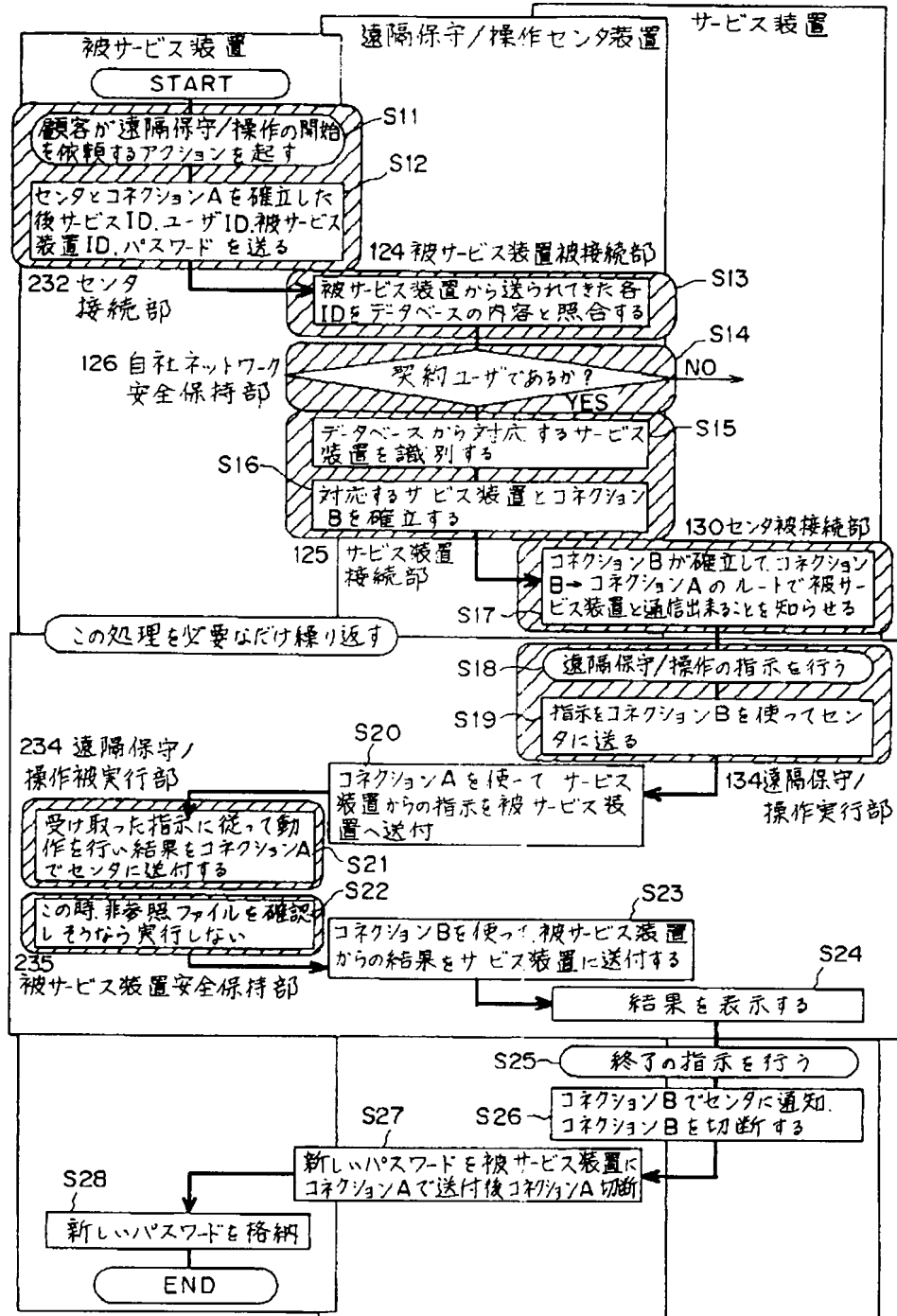


本発明の一実施例である遠隔保守及び遠隔操作を行うシステムの全体構成を示す図



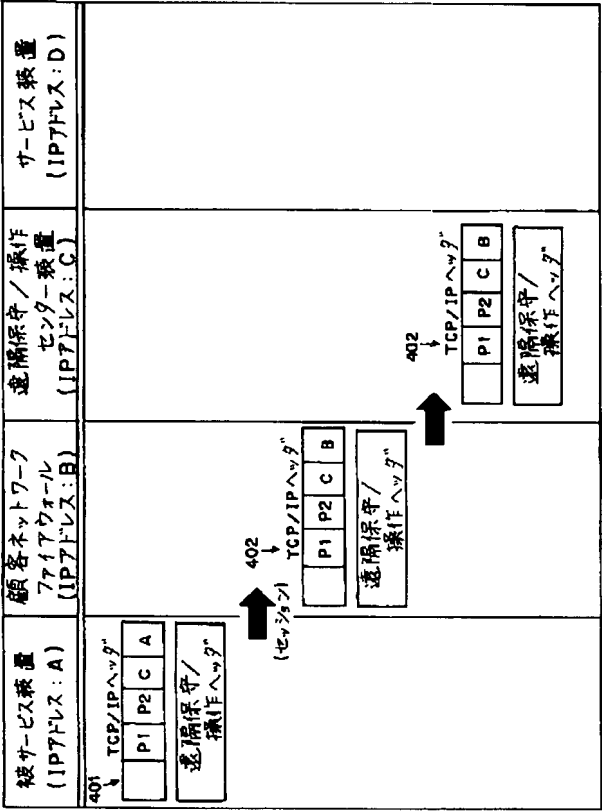
【図6】

実施例の全体動作を説明する図



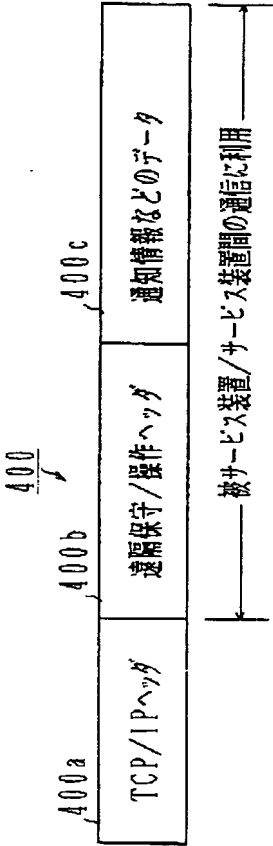
【図9】

図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、両装置間で授受されるパケットの内容を示す図（その1）



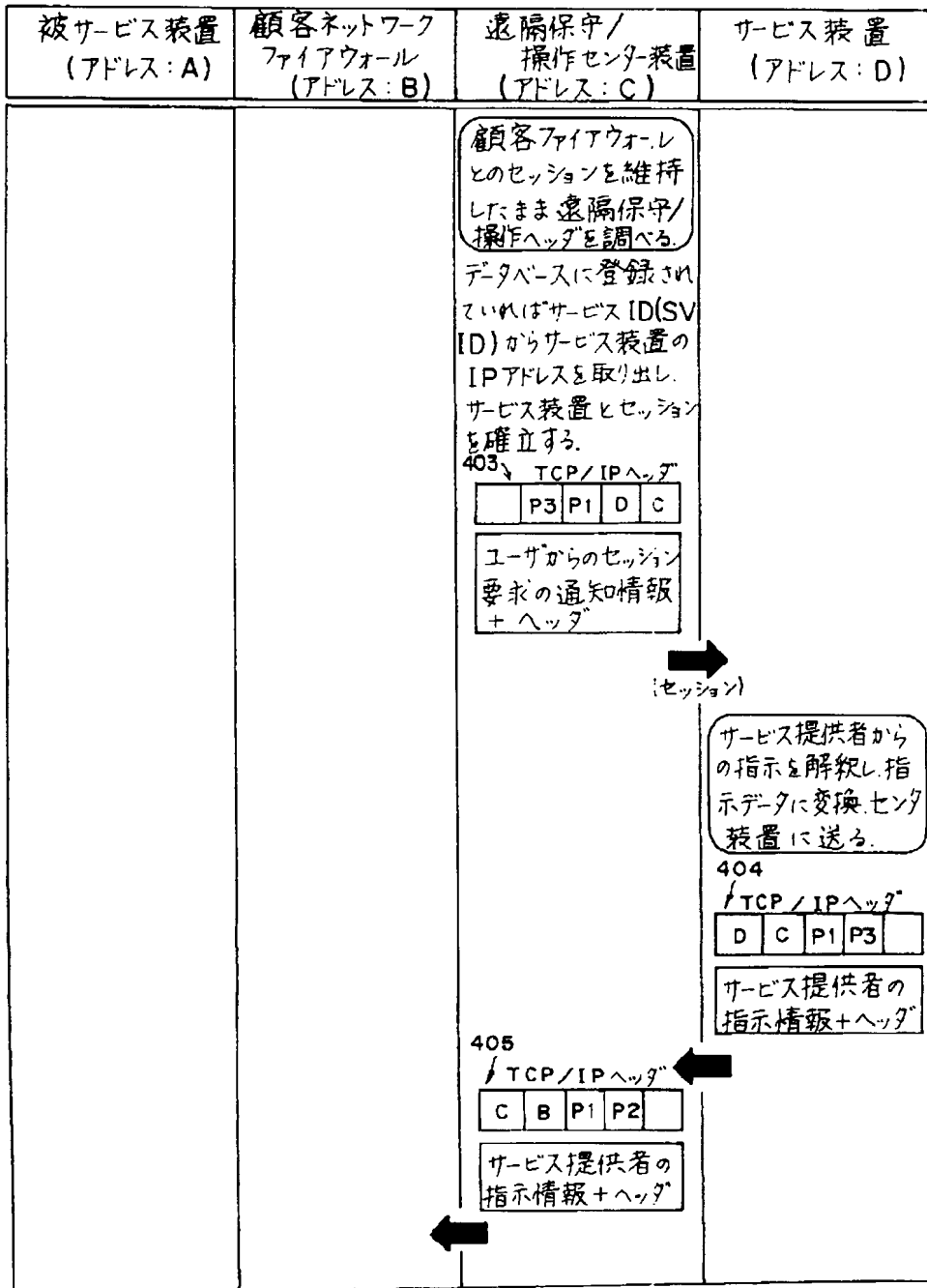
【図12】

図9～図11に示す動作中において、被サービス装置とサービス装置間で送受信されるパケットのフォーマットを示す図



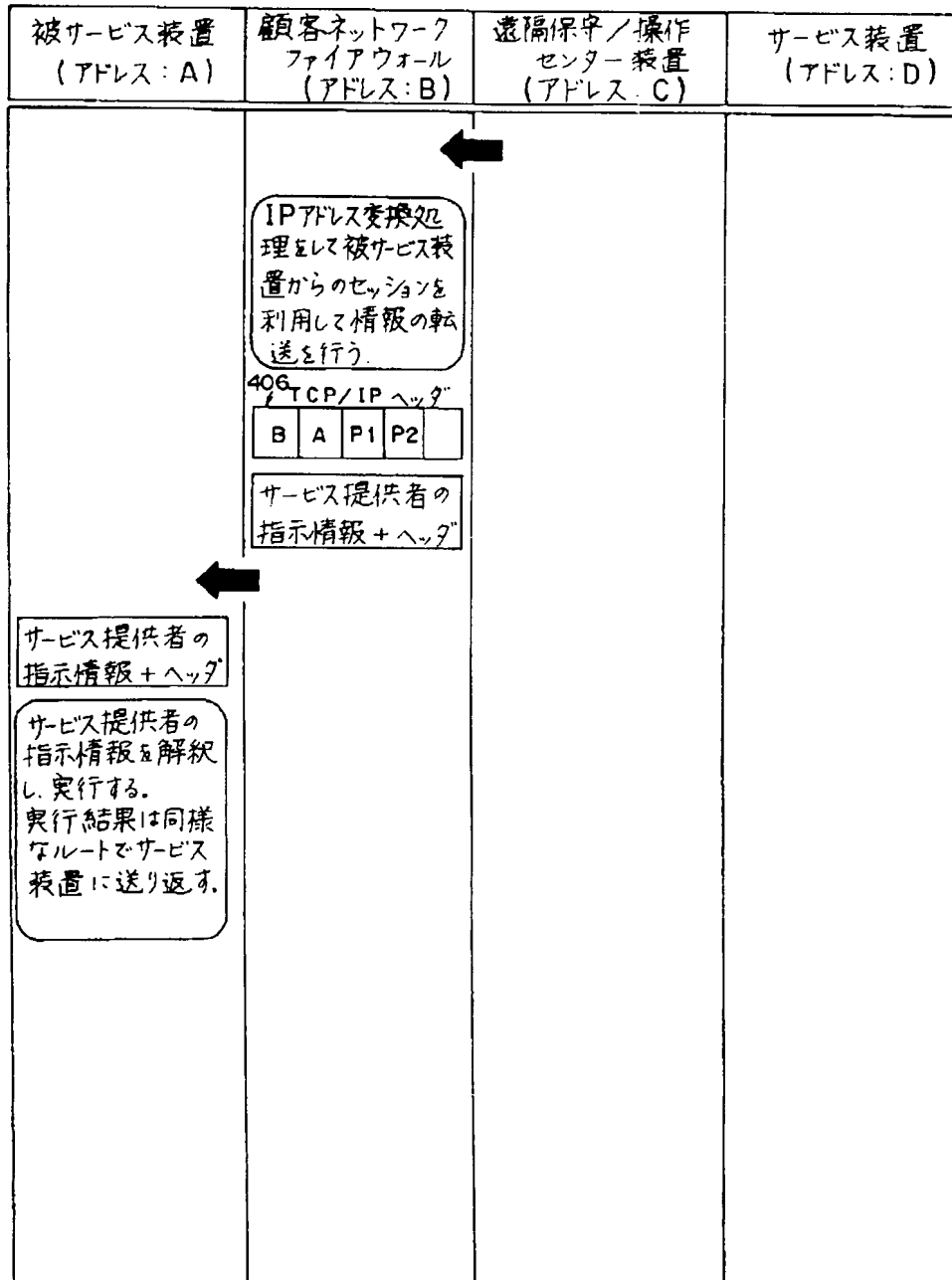
【図10】

図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、両装置間で授受されるパケットの内容を示す図（その2）



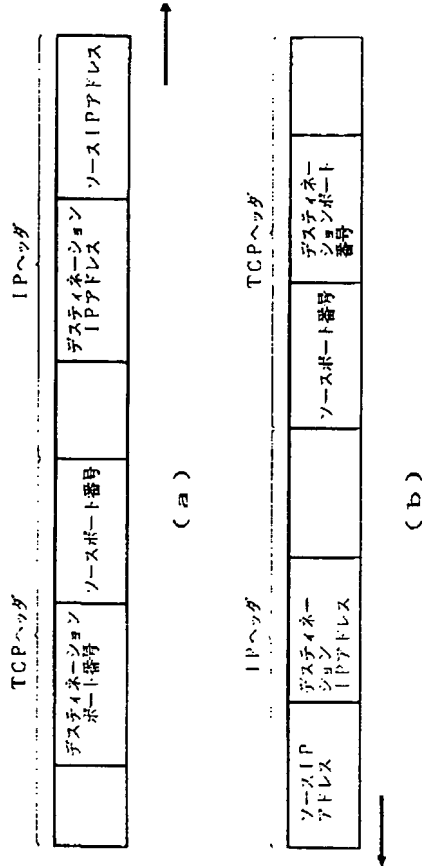
【図11】

図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、両装置間で授受されるパケットの内容を示す図（その3）



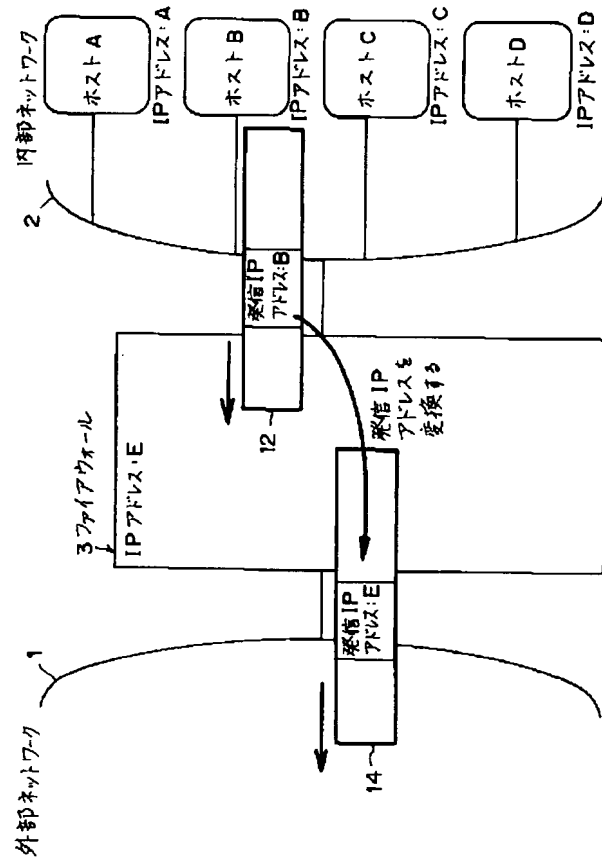
【図13】

図9及び図11に示されたパケットのフォーマットを説明する図



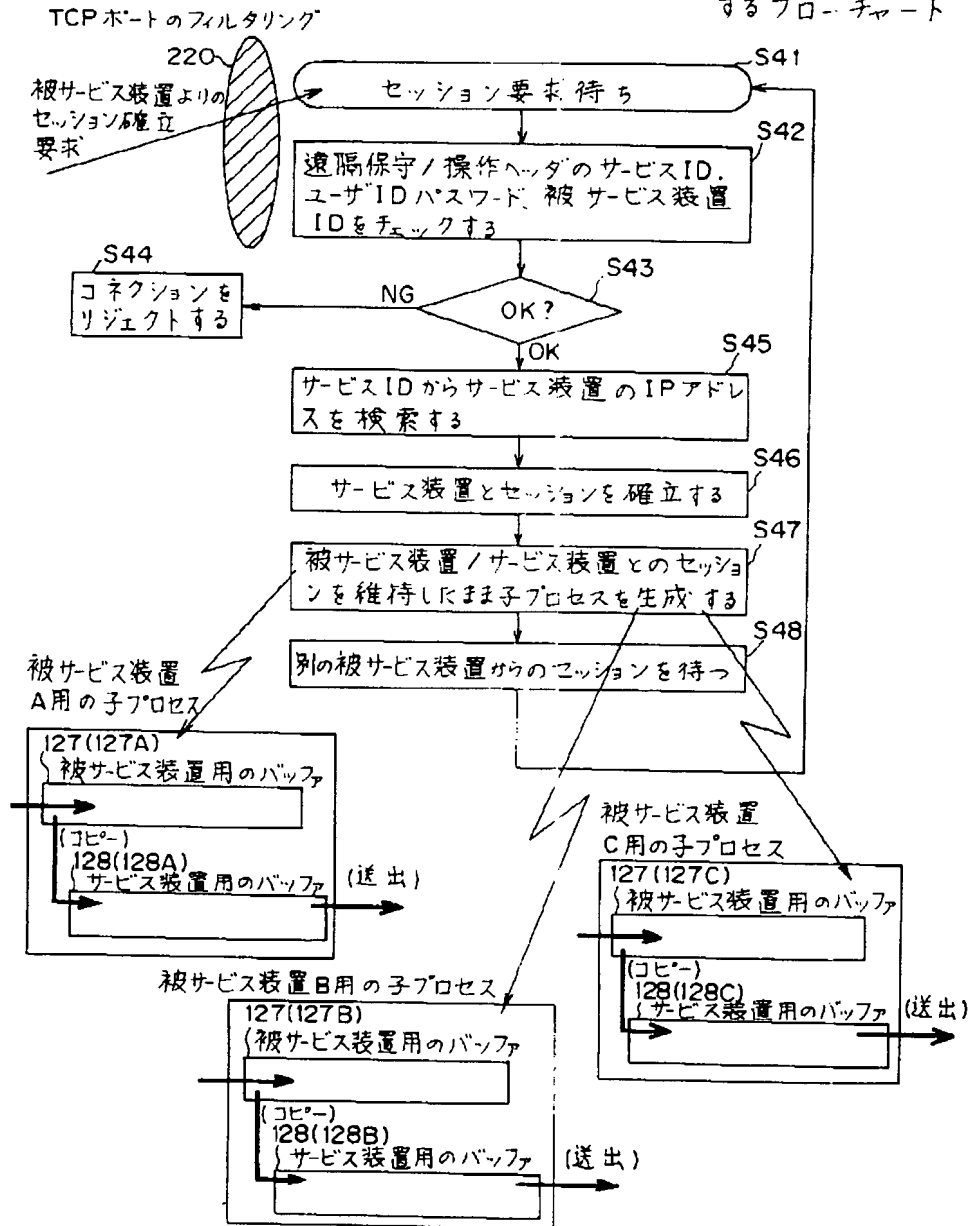
【図17】

ファイアウォールの第二の機能である
IPアドレス変換/中継機能を説明する図



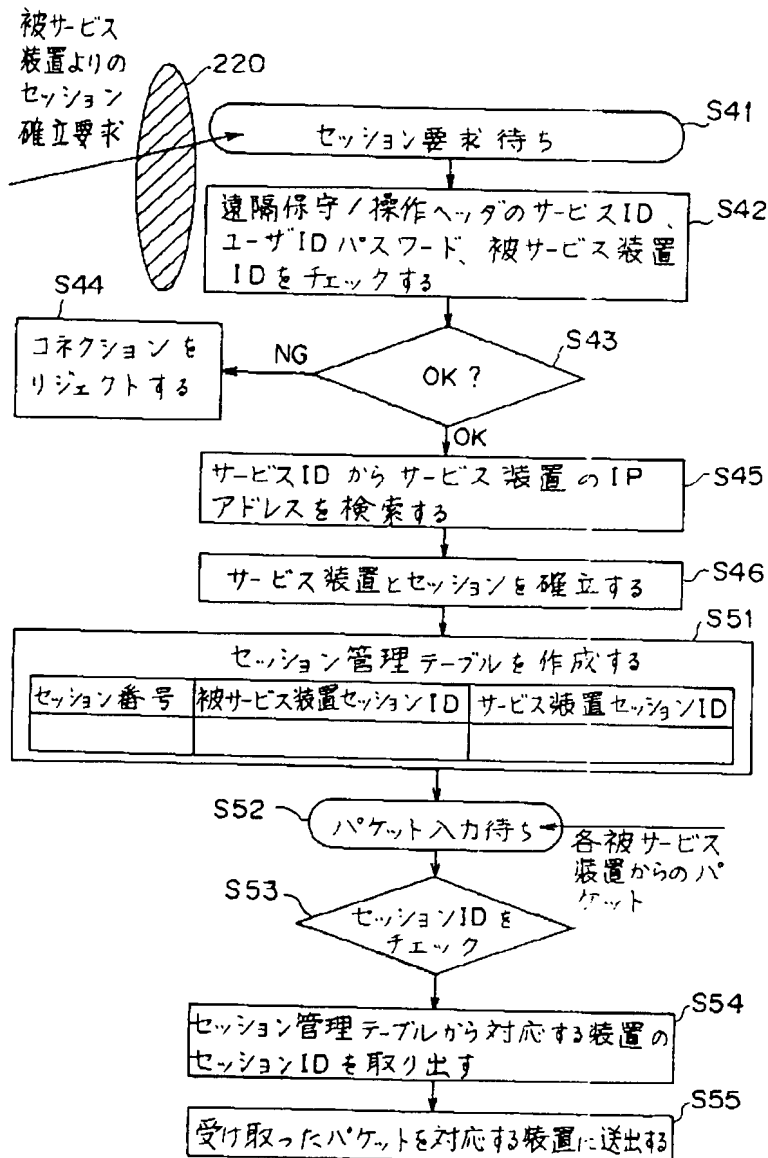
【図14】

遠隔保守／操作センタ装置が被サービス装置とサービス装置との間のパケット(IPデータグラム)の中継処理を実行する動作を説明するフローチャート



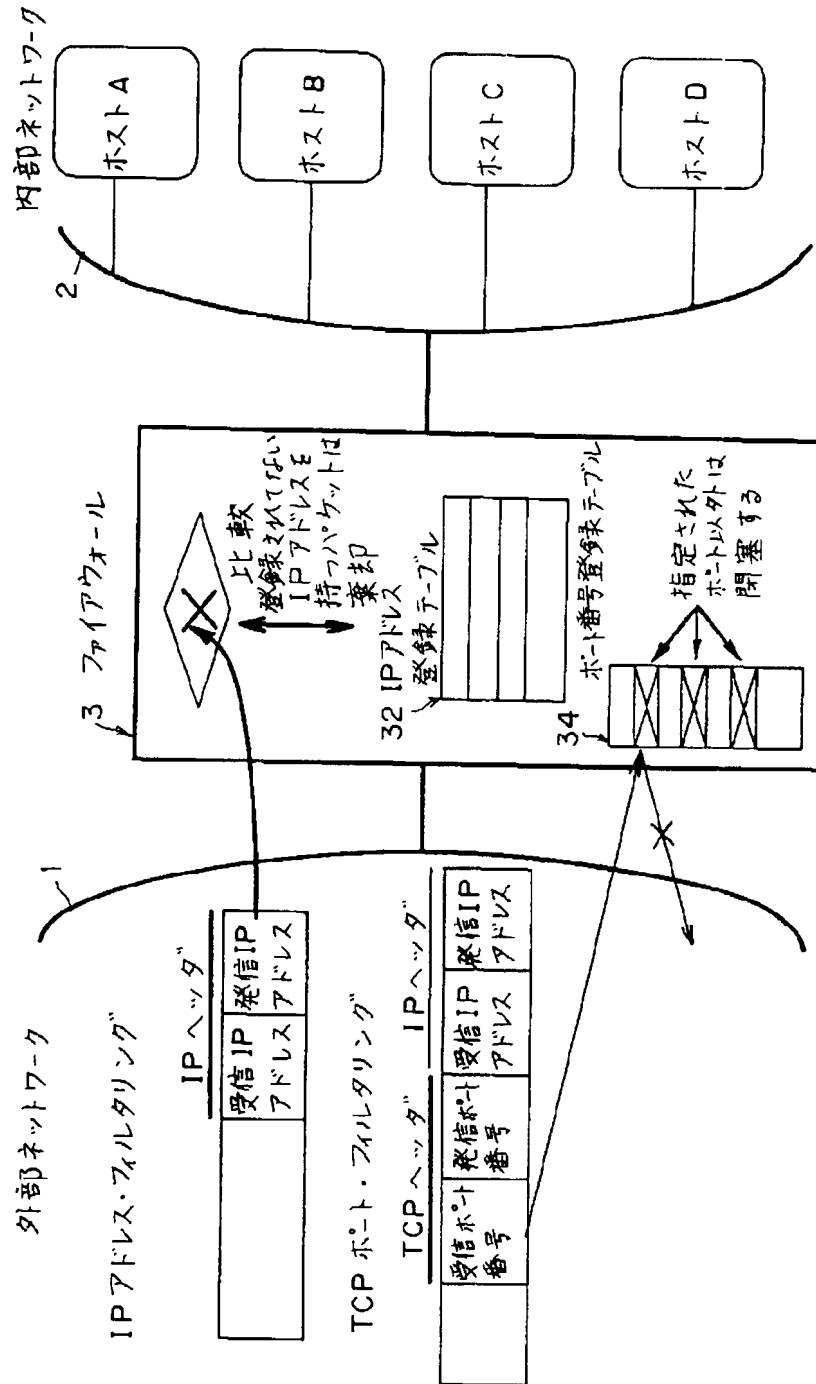
【図15】

図14のフローチャートに示された遠隔保守／操作センタ装置120のIP中継機能を別の観点から説明するフローチャート



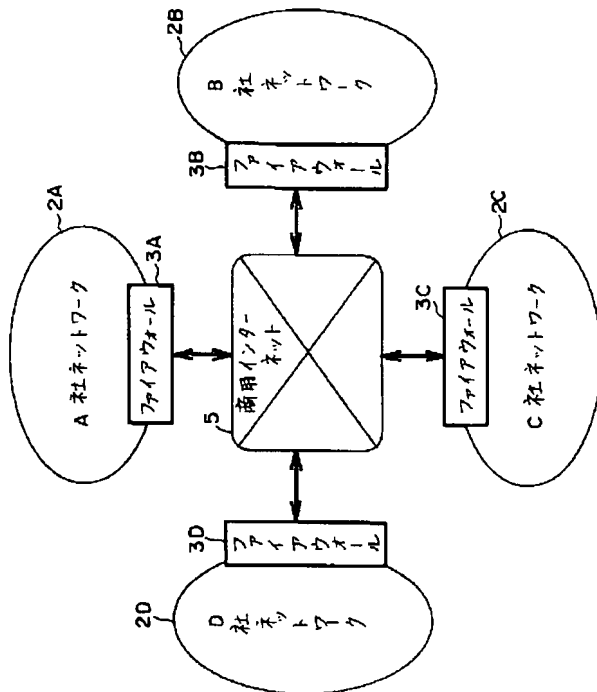
【図16】

ファイアウォールのパケットフィルタリングゲートウェイ機能を説明する図



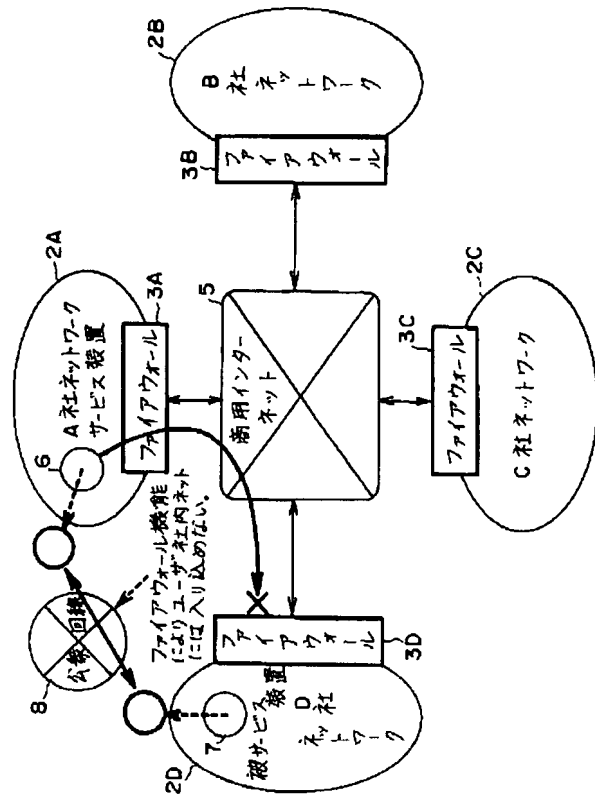
【図18】

A社、B社、C社、及びD社の内部ネットワークがファイアウォールを介して、商用インターネットに接続されたシステムを示す図



【図19】

図18に示すシステムにおいて、A社の内部ネットワークに接続されたサービス装置がD社の内部ネットワークに接続された被サービス装置の遠隔保守／操作を実施できない原因を説明する図



【図20】

図18に示すシステムにおいて、A社の内部ネットワークに接続されたサービス装置がD社の内部ネットワークに接続された被サービス装置の遠隔保守／操作を実施する従来の方法を説明する図

